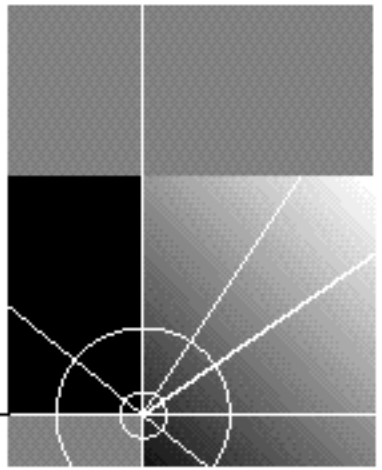
SuperStack® II Switch 3000 FX User Guide

Agent Software Version 3.1



http://www.3com.com/

Document No. DUA1694-0AAA04
Published June 1997

3Com Corporation ■ 5400 Bayfront Plaza ■ Santa Clara, California ■ 95052-8145

Copyright © **3Com Ireland, 1997.** All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without permission from 3Com Ireland.

3Com Ireland reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Ireland to provide notification of such revision or change.

3Com Ireland provides this documentation without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

UNITED STATES GOVERNMENT LEGENDS:
If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following restricted rights:

For units of the Department of Defense:
Restricted Rights Legend: Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) for Restricted Rights in Technical Data and Computer Software Clause at 48 C.F.R. 52.227-7013. 3Com Ireland, c/o 3Com Limited, 3Com Centre, Boundary Way, Hemel Hempstead, Herts, HP2 7YU, United Kingdom.

For civilian agencies:
Restricted Rights Legend: Use, reproduction, or disclosure is subject to restrictions set forth in subparagraph (a) through (d) of the Commercial Computer Software - Restricted Rights Clause at 48 C.F.R. 52.227-19 and the limitations set forth in 3Com Corporation's standard commercial agreement for the software. Unpublished rights reserved under the copyright laws of the United States.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, NetAge, SuperStack, and Transcend are registered trademarks of 3Com Corporation. 3ComFacts is a service mark of 3Com Corporation.

Other brand and product names may be registered trademarks or trademarks of their respective holders.

Environmental Statement

It is 3Com's policy to be environmentally friendly in all its operations. This manual is printed on paper that comes from European sustainable, managed forests. The production process for making the pulp has a reduced AOX level (adsorbable organic halogen) resulting in elemental chlorine free paper.

This paper is fully biodegradable and recyclable.

CONTENTS

ABOUT THIS GUIDE

Introduction 1
How to Use This Guide 1
Conventions 2
Related Documentation 2

1 GETTING STARTED

About the Switch 3000 FX 1-1
- Summary of Features 1-1
- Port Connections 1-2
  - 100BASE-FX Ports 1-2
  - 100BASE-TX Port 1-2
  - Plug-in Module 1-2
  - Transceiver Module 1-2
- Switch Operation and Features 1-3
  - Intelligent Flow Management 1-3
  - Full Duplex 1-3
  - Resilient Links 1-3
  - Virtual LANs 1-4
  - Spanning Tree Protocol 1-4
  - PACE 1-4

Network Configuration Examples 1-6
Unit Overview — Front 1-8
- 100BASE-FX Ports 1-9
- 100BASE-TX Port 1-9
- LEDs 1-9

Unit Overview — Rear 1-10
- Power Socket 1-11
- Unit Serial Number 1-11
- Redundant Power System Socket 1-11
- Reset Button 1-11
- Console Port 1-11
- Plug-in Module Slot 1-11
- Transceiver Module Slot 1-11
- Ethernet Address 1-11

Unit Defaults 1-12
Managing the Switch 3000 FX 1-12
Quick Start For SNMP Users 1-13
- Entering an IP Address for the Switch 1-13

2 INSTALLATION AND SETUP

Following Safety Information 2-1
Positioning the Switch 3000 FX 2-1
Configuration Rules for Fast Ethernet 2-2
Configuration Rules with Full Duplex 2-2
Installing the Switch 3000 FX 2-4
- Rack Mounting 2-4
- Stacking the Switch and Other Units 2-4
- Wall Mounting 2-5

Powering-Up the Switch 2-6
Connecting a Redundant Power System (RPS) 2-6
Connecting Equipment to the Console Port 2-7
- Connecting a VT100 Terminal 2-7

Connecting a VT100 Terminal Emulator 2-7
Connecting a Workstation Running SLIP 2-8

3 SETTING UP FOR MANAGEMENT

Methods of Managing the Switch 3-1
Using the VT100 Management Interface 3-1
Using Telnet 3-2
Managing Over The Network 3-2
IP Addresses 3-2
Obtaining a Registered IP Address 3-3
Navigating the VT100 Screens 3-4
Screen Conventions 3-4
Keyboard Shortcuts 3-5
Correcting Text Entry 3-5
Setting up the Switch for Management 3-6
Logging On 3-7
After Logging On 3-8
Switch Management Setup 3-9
Logging Off 3-12
Auto Logout 3-12

4 MANAGING THE SWITCH 3000 FX

Setting Up Users 4-2
Creating a New User 4-3
Deleting a User 4-4
Editing User Details 4-5
Assigning Local Security 4-6
Choosing a Switch Management Level 4-7
Setting Up the Switch Unit 4-9
Setting Up the Switch Ports 4-11
Setting Up the Switch Database (SDB) 4-15
The Database View 4-16
Searching the Switch Database 4-17
By MAC Address 4-17
By Port 4-17
Adding an Entry into the SDB 4-17
Deleting an Entry from the SDB 4-17
Specifying that an Entry is Permanent 4-17
Setting Up Resilient Links 4-18
Configuring Resilient Links 4-19
Creating a Resilient Link Pair 4-20
Deleting a Resilient Link Pair 4-20
Viewing the Resilient Setup 4-21
Setting Up Traps 4-23
Setting Up the Console Port 4-24
Resetting the Switch 3000 FX 4-26
Initializing the Switch 3000 FX 4-27
Upgrading Software 4-28

5 ADVANCED MANAGEMENT

Virtual LANs (VLANs) 5-1
What are VLANs? 5-1
Benefits of VLANs 5-1
How VLANs Ease Change and Movement 5-2
How VLANs Control Broadcast Traffic 5-2
How VLANs Provide Extra Security 5-2
An Example 5-2
VLANs and the Switch 3000 FX 5-3
The Default VLAN and Moving Ports From the Default VLAN 5-3
Connecting VLANs to a Router 5-3
Connecting Common VLANs Between Switch Units 5-3
Using AutoSelect VLAN Mode 5-4
Using Non-routable Protocols 5-5
Using Unique MAC Addresses 5-5

Extending VLANs into an ATM Network 5-5
VLAN Configuration Example 5-6
Setting Up VLANs on the Switch 5-8
Assigning a Port to a VLAN When Using Port VLAN Mode 5-9
Specifying that a Port is a VLT Port 5-9
Setting Up VLANs Using AutoSelect VLAN Mode 5-10
Specifying Information About the VLAN Server 5-10
Specifying AutoSelect VLAN Mode 5-11
Spanning Tree Protocol 5-12
What is STP? 5-12
How STP Works 5-14
STP Initialization 5-14
STP Stabilization 5-14
STP Reconfiguration 5-14
An Example 5-15
STP Configurations 5-16
Enabling STP on the Switch 5-17
Configuring STP on the Switch 5-18
Configuring the STP Parameters of VLANs 5-18
Configuring the STP Parameters of Ports 5-20
RMON 5-22
What is RMON? 5-22
About the RMON Groups 5-22
Statistics 5-22
History 5-22
Alarms 5-23
Hosts 5-23
Hosts Top N 5-23
Matrix 5-23
Filter 5-23
Capture 5-23
Events 5-24
Benefits of RMON 5-24
RMON and the Switch 5-25
RMON Features of the Switch 5-25
About Alarm Actions 5-27
About Default Alarm Settings 5-28
About the Audit Log 5-28

6 STATUS MONITORING AND STATISTICS

Summary Statistics 6-2
Port Statistics 6-3
Port Traffic Statistics 6-4
Port Error Analysis 6-6
Status Monitoring 6-8
Fault Log 6-9
Remote Polling 6-10

A SAFETY INFORMATION

Important Safety Information A-1
Power Supply and Fuse A-3
Sockets for Redundant Power System (RPS) A-3
RJ45 Ports A-3
Fiber Ports A-3
L'information de Sécurité Importante A-4
La Source de Courant et Le Fusible A-5
Socle Pour Alimentation Multiple A-6
Les Ports RJ45 A-6
Les Ports Fibre A-6
Wichtige Sicherheitsinformationen A-7
Stromversorgung und Sicherung A-8
Steckdose für Redundant Power System (RPS) A-8
RJ45 Anschlußen A-8
Glasfaser Anschlußen A-9

B SCREEN ACCESS RIGHTS

C TROUBLE-SHOOTING

LEDs C-1
Using the VT100 Interface C-2
Using the Switch C-3

D PIN-OUTS

Null Modem Cable D-1
PC-AT Serial Cable D-1
Modem Cable D-2
RJ45 Pin Assignments D-2

E SWITCH 3000 FX TECHNICAL SPECIFICATIONS

F TECHNICAL SUPPORT

Online Technical Services F-1
- World Wide Web Site F-1
- 3Com Bulletin Board Service F-1
  - Access by Analog Modem F-1
  - Access by Digital Modem F-2
- 3ComFacts Automated Fax Service F-2
- 3ComForum on CompuServe Online Service F-2

Support from Your Network Supplier F-3
Support from 3Com F-3
Returning Products for Repair F-4

GLOSSARY

INDEX

3COM CORPORATION LIMITED WARRANTY

ELECTRO-MAGNETIC COMPATIBILITY STATEMENTS

About This Guide

About This Guide provides an overview of this guide, describes the guide conventions, tells you where to look for specific information and lists other publications that may be useful.

Introduction

This guide provides the information you need to install and configure a Switch 3000 FX (3C16940A) with v3.1 agent software. The guide is intended for use by network administrators who are responsible for installing and setting up network equipment; consequently, it assumes a basic working knowledge of Local Area Networks.

If the information in the Release Notes shipped with your product differs from the information in this guide, follow the Release Notes.

Throughout this guide, the SuperStack® II Switch 3000 FX is referred to as the Switch 3000 FX or Switch.

How to Use This Guide

This table shows where to find specific information in this guide.

If you are looking for...	Turn to...
An overview of the Switch 3000 FX	Chapter 1
Information about installing the Switch 3000 FX into your network	Chapter 2
Information about the methods you can use to manage the Switch 3000 FX	Chapter 3
Information about managing the Switch 3000 FX	Chapter 4
Information about more advanced management features; for example VLANs, Spanning Tree and RMON	Chapter 5
Information about monitoring the status of the Switch 3000 FX	Chapter 6
Safety information	Appendix A
Information about the access rights for each VT100 screen	Appendix B
Trouble-shooting information	Appendix C
Information about the pin-outs relating to the Switch 3000 FX	Appendix D
Information about the Technical Specifications of the Switch 3000 FX	Appendix E
Information about the Technical Support available from 3Com	Appendix F

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1 Text Conventions

Convention	Description
`Screen displays`	This typeface represents information as it appears on the screen.
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."
[Key] names	Key names appear in text in one of two ways: ■ Referred to by their labels, such as "the Return key" or "the Escape key" ■ Written with brackets, such as [Return] or [Esc]. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del].
Menu commands and *buttons*	Menu commands or button names appear in italics. Example: From the *Help* menu, select *Contents*.
Words in *italicized* type	Italics emphasize a point or denote new terms at the place where they are defined in the text.
Words in **bold-face** type	Bold text denotes key features.

Table 2 Notice Icons

Icon	Notice Type	Alerts you to...
	Information note	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Related Documentation

The Switch 3000 FX document set includes:

- *SuperStack II Switch 3000 FX Quick Reference Guide*.
  Document Number DQA1694-0AAA0x
- *SuperStack II Switch 3000 FX Quick Installation Guide*.
  Document Number DIA1694-0AAA0x
- *SuperStack II Switch 3000 FX Release Notes*.
  Document Number DNA1694-0AAA0x

Other publications you may find useful:

- Documentation accompanying the Plug-in Modules.
- Documentation accompanying the Redundant Power System.

1 GETTING STARTED

About the Switch 3000 FX

Switching is currently a leading option for increasing performance by providing high speed backbone links and eliminating server bottlenecks. Part of the 3Com SuperStack® II range of products, the Switch 3000 FX provides simple, low cost and high performance switched connections to Fast Ethernet networks.

The SuperStack II Switch 3000 FX is a revision of the LinkSwitch 3000.

Summary of Features

The Switch 3000 FX has the following features:

- Five 100BASE-FX ports and one 100BASE-TX port
- Plug-in Module slot (Asynchronous Transfer Mode (ATM) and Fast Ethernet)
- Transceiver Module slot (10Mbps Ethernet)
- Support for up to 4080 addresses in the Switch Database
- *Store-and-forward* forwarding mode ensuring the switch forwards all valid Ethernet frames and discards invalid Ethernet frames such as those with an incorrect CRC
- Intelligent Flow Management for congestion control
- Full duplex on all fixed ports, and Fast Ethernet Plug-in Module ports
- Resilient Links
- Support for 16 Virtual LANs (VLANs)
- Spanning Tree Protocol (STP) per VLAN
- PACE (Priority Access Control Enabled) for supporting multimedia applications over Ethernet
- 3Com's SuperStack II architecture:
  - Connects to Redundant Power System
  - Integrated network management
  - 19-inch rack or stand-alone mounting
- SmartAgent support:
  - IP and IPX management over SNMP
  - RMON
  - Repeater and Bridge MIB
  - Broadcast storm control
  - Easy software upgrades
  - BOOTP for automatic IP address configuration
  - Local management

Port Connections

100BASE-FX Ports

The Switch has five Fast Ethernet 100BASE-FX ports, which provide connection to Fast Ethernet devices such as the SuperStack II Switch 1000 with a 100BASE-FX Plug-in Module. Use 100BASE-FX fiber optic cable with SC connectors to support switching over 62.5/125 micron. The maximum distance supported is 412m (1352ft).

The maximum distance supported can be extended to 2km (6562ft) with full duplex. For more information, refer to "Full Duplex" on page 1-3.

100BASE-TX Port

The Switch has a single Fast Ethernet 100BASE-TX port configured as MDIX (cross-over), which provides a 100Mbps connection to, for example, a local server. The maximum segment length is 100m (328ft) over grade 5 twisted pair cable.

As this port is configured as MDIX (cross-over), you need to use a cross-over cable to connect to devices whose ports are MDIX-only. Most of the 100BASE-TX ports in 3Com devices are MDIX-only.

Plug-in Module

A slot at the rear of the unit can take a Plug-in Module, providing an additional high-speed port. This could be used for example, to provide a Fast Ethernet or Asynchronous Transfer Mode (ATM) backbone connection to the rest of your network.

Transceiver Module

A slot at the rear of the unit allows you to install any of the 3Com 10Mbps Ethernet Transceiver Modules. The Transceiver Module can provide a 10Mbps link to the rest of your network.

Switch Operation and Features

The Switch 3000 FX uses the same algorithm as a conventional 802.1d bridge for filtering, forwarding and learning packets.

Intelligent Flow Management

Intelligent Flow Management (IFM) is a system for controlling congestion on your network. Congestion can be caused by one or more devices sending traffic to an already busy port on the Switch 3000 FX. If a port on the Switch 3000 FX is connected to another switch or endstation, IFM prevents packet loss and inhibits the device from generating more packets until the period of congestion ends.

IFM should be enabled on a port if it is connected to another switch, or an endstation. IFM should be disabled on a port connected to a repeater.

For more information about enabling IFM on a port, refer to "Setting Up the Switch Ports" on page 4-11.

Full Duplex

The Switch 3000 FX provides full duplex support for all its fixed ports, and Fast Ethernet Plug-in Module ports. Full duplex allows frames to be transmitted and received simultaneously and, in effect, doubles the potential throughput of a link. In addition, full duplex also supports 100BASE-FX cable runs of up to 2km (6562ft).

Full duplex can be enabled on all the relevant ports, or on individual ports. Full duplex is not supported by the Transceiver Module.

For more information about enabling full duplex, refer to "Setting Up the Switch Unit" and "Setting Up the Switch Ports" in Chapter 4.

Resilient Links

The Resilient Link feature in the Switch 3000 FX enables you to protect critical links and prevent network downtime should those links fail. Setting up resilience ensures that should a main communication link fail, a standby duplicate link immediately and automatically takes over the task of the main link. Each main and standby link pair is referred to as a resilient link pair.

For more information about resilient links, refer to "Setting Up Resilient Links" on page 4-18.

Virtual LANs

The Switch 3000 FX has a Virtual LAN (VLAN) feature which allows you to build your network segments without being restricted by physical connections. A VLAN is defined as a group of location- and topology-independent devices that communicate as if they are on the same physical LAN.

Implementing VLANs on your network has three main advantages:

- It eases the change and movement of devices on IP networks. If an endstation in VLAN 1 is moved to a port in another part of the network, you only need to specify that the new port is in VLAN 1.
- It helps to control broadcast traffic. If an endstation in VLAN 1 transmits a broadcast frame, then only VLAN 1 devices receive the frame.
- It provides extra security. Devices in VLAN 1 can only communicate with devices in VLAN 2 using a router.

For more information about VLANs, refer to "Virtual LANs (VLANs)" on page 5-1.

Spanning Tree Protocol

The Switch 3000 FX supports the Spanning Tree Protocol (STP) which is a bridge-based system for providing fault tolerance on networks. STP allows you to implement parallel paths for network traffic, and ensure that:

- Redundant paths are disabled when the main paths are operational.
- Redundant paths are enabled if the main traffic paths fail.

For more information about STP, refer to "Spanning Tree Protocol" on page 5-12.

PACE

The Switch 3000 FX supports PACE (Priority Access Control Enabled) technology, which allows multimedia traffic to be carried over standard Ethernet and Fast Ethernet LANs. PACE provides two features:

- *Implicit Class of Service* — When multimedia traffic is transmitted, it is given a higher priority than other data and is therefore forwarded ahead of other data when it arrives at the Switch. The Implicit Class of Service feature minimizes latency through the Switch and protects the quality of multimedia traffic.

- *Interactive Access* — When two-way multimedia traffic passes over an Ethernet network, interference can occur because access to the bandwidth is unequally allocated to traffic in one direction. The Interactive Access feature allocates the available bandwidth equally in both directions, therefore increasing the quality of the traffic.

For more information about setting up PACE on the Switch, refer to "Setting Up the Switch Unit" and "Setting Up the Switch Ports" in Chapter 4.

Network Configuration Examples

The following two illustrations show some examples of how the Switch 3000 FX can be used on your network.

Examples of how the Switch 3000 FX can be used in a VLAN-based network are given in Chapter 5.

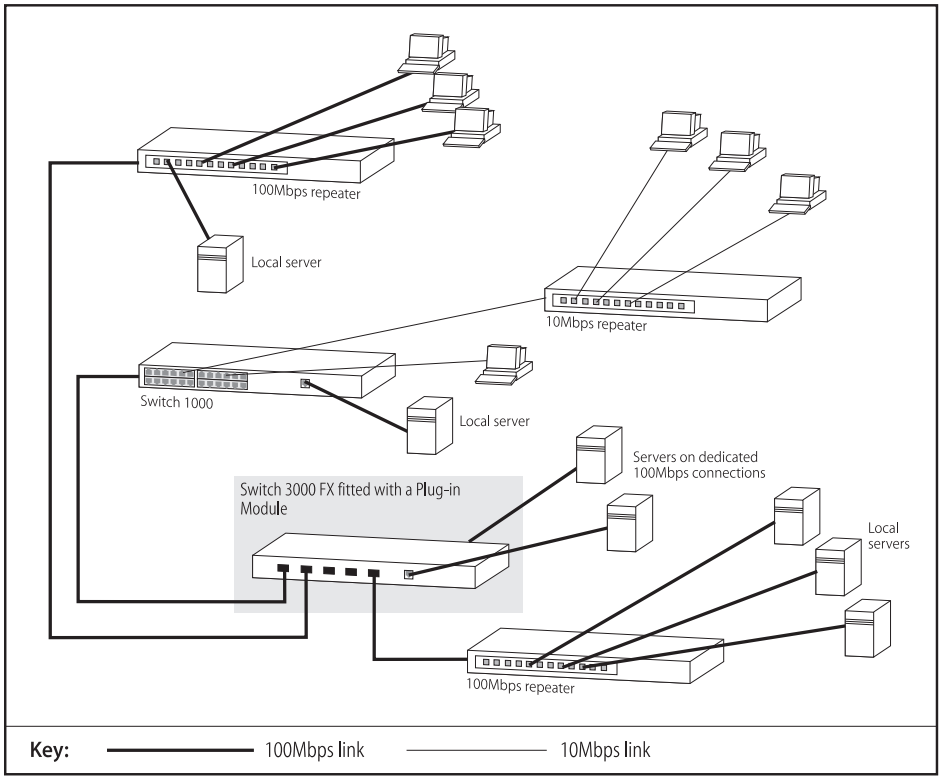


Figure 1-1 The Switch 3000 FX used as a data-center switch

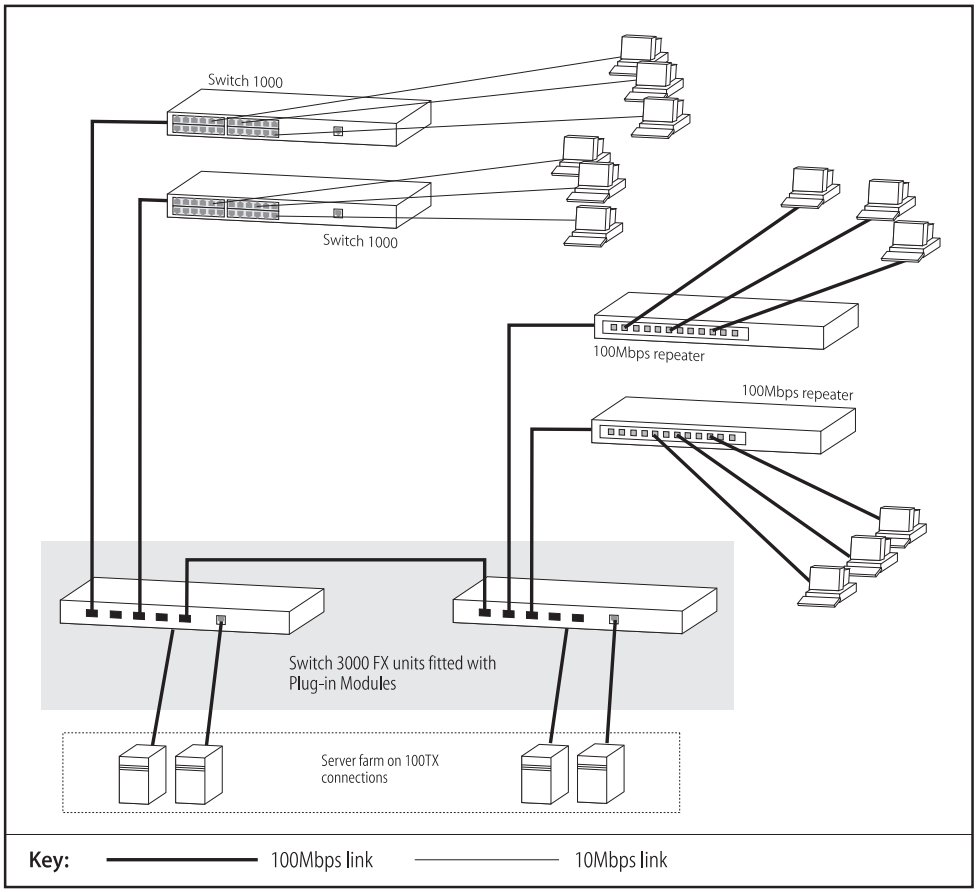


Figure 1-2 Increasing port density with the Switch 3000 FX

Unit Overview — Front

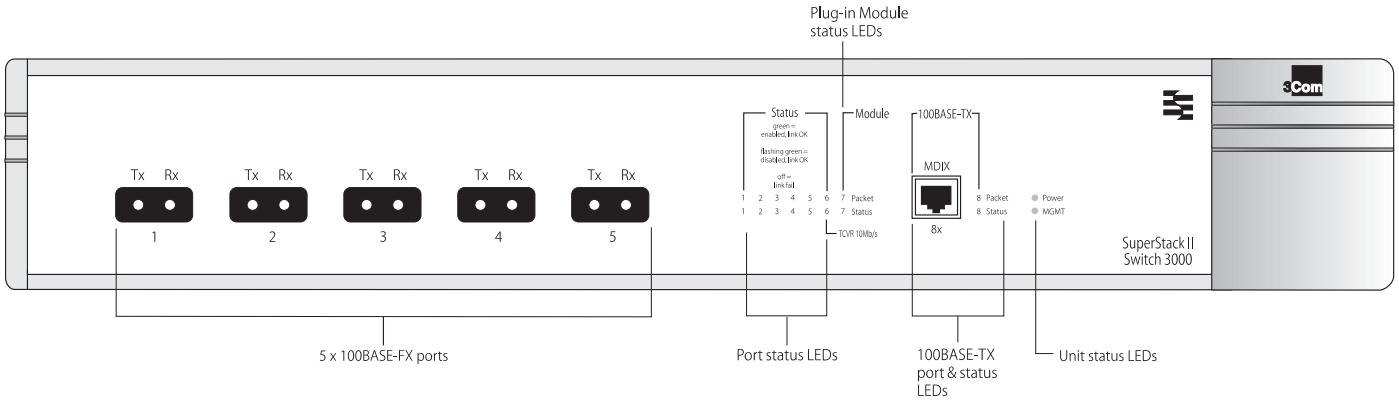


Figure 1-3 Switch 3000 FX front view

100BASE-FX Ports

The Switch has five Fast Ethernet 100BASE-FX ports, which provide connection to Fast Ethernet devices such as the SuperStack II Switch 1000 with a 100BASE-FX Plug-in Module. Use 100BASE-FX fiber optic cable with SC connectors to support switching over 62.5/125 micron. The maximum distance supported is 412m (1352ft).

The maximum distance supported can be extended to 2km (6562ft) with full duplex. For more information, refer to "Full Duplex" on page 1-3.

100BASE-TX Port

The Switch has a single Fast Ethernet 100BASE-TX RJ45 port configured as MDIX (cross-over), which provides a 100Mbps connection to, for example, a local server. Maximum segment length is 100m (328ft) over category 5 UTP or STP cable.

As this port is configured as MDIX (cross-over), you need to use a cross-over cable to connect to devices whose ports are MDIX-only. Most of the 100BASE-TX ports in 3Com devices are MDIX-only.

LEDs

The table below describes the LED behavior on the Switch 3000 FX. For more details about corrective action in the event of a problem, refer to "LEDs" on page C-1.

LED	Color	Indicates
Port Status LEDs (ports 1–6 and 8)		
Packet	Yellow	Frames are being transmitted/received on the port.
Status	Green	Link is present; port is enabled.
	Green flashing	Link is present; port is disabled.
	Off	Link is not present.
Plug-in Module Status LEDs (port 7)		
Packet	Yellow	Frames are being transmitted/received on the Plug-in Module port.
Status	Green	Link is present; port is enabled.
	Green flashing	Link is present; port is disabled.
	Green flashing (long on, short off)	Refer to the "*SuperStack II Switch ATM OC-3c Module User Guide*".
	Yellow	Plug-in Module has failed its Power On Self Test (if the MGMT LED is flashing yellow), or the agent software of the Plug-in Module is not installed correctly.
	Yellow flashing	Plug-in Module is not recognized.
	Off	Link is not present or Plug-in Module is not installed in the Switch.
Unit Status LEDs		
Power	Green	Switch is powered-up.
MGMT	Green	Switch is operating normally.
	Green flashing	Switch or Plug-in Module is either downloading software or initializing (which includes a Power On Self Test).
	Yellow	Switch has failed its Power On Self Test.
	Yellow flashing	Plug-in Module has failed its Power On Self Test.

Unit Overview — Rear

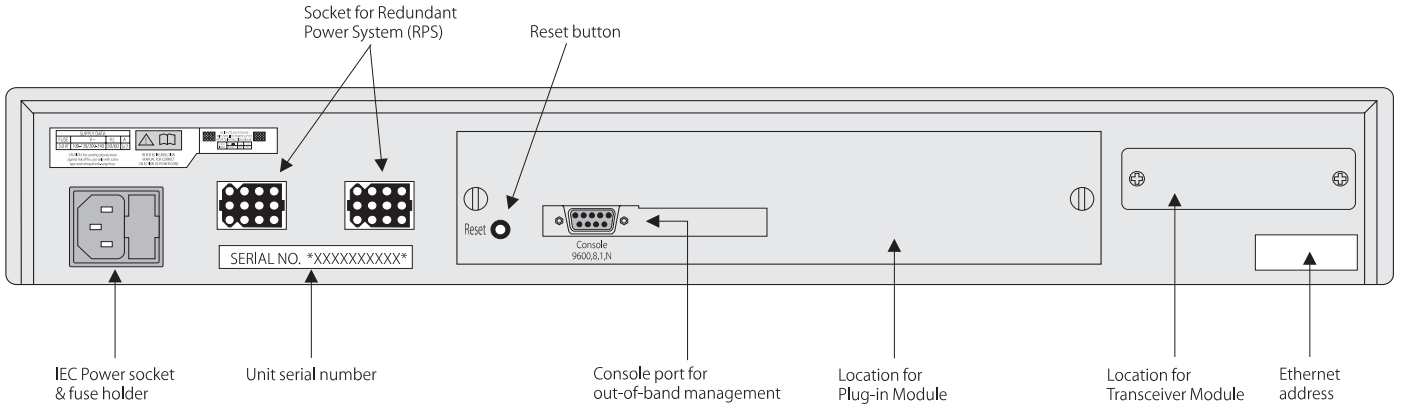


Figure 1-4 Switch 3000 FX rear view

Power Socket

The Switch 3000 FX automatically adjusts to the supply voltage. The fuse is suitable for both 110V A.C. and 220–240V A.C. operation. For information on replacing fuses, refer to Appendix A.

Unit Serial Number

You may need this serial number for fault reporting purposes.

Redundant Power System Socket

Use one of these sockets to connect a SuperStack II Redundant Power System (RPS) to the unit. You can use either socket. Refer to "Connecting a Redundant Power System (RPS)" on page 2-6.

Reset Button

Using the reset button simulates a power-off/on cycle. This has the same effect as carrying out a reset via the VT100 interface; refer to "Resetting the Switch 3000 FX" on page 4-26.

Console Port

Connect a terminal to the console port to carry out remote or local out-of-band configuration and management. The console port is set to auto-baud, 8 data bits, no parity, and 1 stop bit.

Plug-in Module Slot

Use this slot to install a Plug-in Module. The Module can be used to provide an additional high speed link to the rest of your network. 3Com provides a range of Plug-in Modules; contact your supplier for availability.

When a Plug-in Module is not installed, ensure the blanking plate is secured in place.

Transceiver Module Slot

Use this slot to connect a Transceiver Module and provide a 10Mbps link to the rest of the network. 3Com provides a range of Transceiver Modules; contact your supplier for availability.

When a Transceiver Module is not installed, ensure the blanking plate is secured in place.

Ethernet Address

This label shows the unique Ethernet (or MAC) address assigned to the unit.

Unit Defaults

The following table shows the factory defaults for the Switch 3000 FX features.

Port Status	Enabled
Intelligent Flow Management	Enabled
Duplex Mode	Half duplex on all relevant ports
Virtual LANs	All ports use Port VLAN Mode and belong to the Default VLAN (VLAN 1)
PACE	Disabled
Spanning Tree (STP)	Disabled
Power On Self Test (POST)	Normal (Fast Boot)
System Alarm (broadcast bandwidth used)	Enabled ■ High threshold: 20% — Notify and Blip ■ Low threshold: 10% — No action
System Alarm (errors per 10,000 packets)	Enabled ■ High threshold: 2% — Notify ■ Low threshold: 1% — No action
System Alarm (bandwidth used)	Enabled ■ High threshold: 85% — No action ■ Low threshold: 50% — No action
System Alarm (percentage of frames forwarded)	Enabled ■ High threshold: 85% — No action ■ Low threshold: 50% — No action

Managing the Switch 3000 FX

The menu-driven interface built into the Switch 3000 FX is known as the VT100 interface. You can access it using a VT100 terminal, or a PC using terminal emulation software. You can connect the terminal directly to the Switch or via a modem. You can also access the VT100 interface remotely using Telnet running over the TCP/IP protocol.

Remote management is also possible using a Network Manager from 3Com's Transcend® product range. The management protocol is SNMP (Simple Network Management Protocol) and any SNMP-based management facility can manage the unit if the Management Information Base (MIB) is installed correctly in the management workstation. The Switch 3000 FX supports SNMP over both IP and IPX protocols.

Quick Start For SNMP Users

This section describes how to get started if you wish to use an SNMP Network Manager to manage the Switch. It assumes you are already familiar with SNMP management.

- If you are using IP and you have a BOOTP server set up correctly on your network, the IP address for the Switch is detected automatically and you can start managing the Switch without any further configuration.
- If you are using the IPX protocol, the Switch 3000 FX is allocated an IPX address automatically. You can start the SNMP Network Manager and begin managing the Switch.
- If you are using IP without a BOOTP server, you must enter the IP address of the Switch before the SNMP network manager can communicate with the device. To do this, refer to "Entering an IP Address for the Switch" below.

If you need more information about IP and IPX, refer to "Managing Over The Network" on page 3-2.

Entering an IP Address for the Switch

1. Connect a terminal to the console port of the Switch 3000 FX, refer to "Connecting a VT100 Terminal" on page 2-7. The terminal should be configured to 9600 line speed (baud rate), 8 data bits, no parity, and 1 stop bit.
2. Press [Return] one or more times until the Main Banner screen is displayed.
3. At the Main Banner screen, press [Return] to display the Logon screen. Log on using the default user name *admin* (no password is required). Select OK.
4. The Main Menu is displayed. From this menu, select the MANAGEMENT SETUP option. The Switch Management Setup screen is displayed.
5. On the Management Setup screen, fill in the following fields:
   - Device IP Address
   - Device SubNet Mask (if necessary)
   - Default Router (if necessary)

   For further information on the Management Setup screen, refer to "Setting up the Switch for Management" on page 3-6.
6. If you need the Switch 3000 FX to send SNMP traps to the Network Manager, you may need to set up the address of the Network Manager in the Trap Table. Refer to "Setting Up Traps" on page 4-23.

3Com Network Managers such as Transcend Work-Group Manager for Windows may automatically configure the Switch 3000 FX to send traps to them. Please read the documentation supplied with your network management software.

7. When you have finished with the Management Setup screen, select OK.

2 INSTALLATION AND SETUP

Following Safety Information

Before installing or removing any components from the Switch or carrying out any maintenance procedures, you must read the safety information provided in Appendix A of this guide.

Positioning the Switch 3000 FX

The Switch is suited for use in the office where it can be wall-mounted, mounted in a standard 19-inch equipment rack, or free standing. Alternatively, the unit can be rack-mounted in a wiring closet or equipment room. A wall-mounting / rack-mounting kit, containing two mounting brackets and six screws, is supplied with the Switch.

When deciding where to position the unit, ensure that:

- You are able to meet the configuration rules detailed in the following section.
- The unit is accessible and cables can be connected easily.
- Cabling is away from:
  - Sources of electrical noise such as radios, transmitters and broadband amplifiers.
  - Power lines and fluorescent lighting fixtures.
- Water or moisture cannot enter the case of the unit.
- Air-flow around the unit and through the vents in the side of the case is not restricted. We recommend that you provide a minimum 25mm (1in.) clearance.
- No objects are placed on top of the unit.
- Units are not stacked more than four high if free-standing.

Configuration Rules for Fast Ethernet

The topology rules for 100Mbps Fast Ethernet are slightly different to those for 10Mbps Ethernet. Figure 2-1 illustrates the key topology rules and provides examples of how they allow for large-scale Fast Ethernet networks.

The key topology rules are:

- Maximum UTP cable length is 100m (328ft) over category 5 cable.
- A 412m (1352ft) fiber run is allowed for connecting switch to switch, or endstation to switch, using half-duplex 100BASE-FX.
- A total network span of 325m (1066ft) is allowed in single-repeater topologies (one hub stack per wiring closet with a fiber run to the collapsed backbone). For example, a 225m (738ft) fiber downlink from a repeater to a router or switch, plus a 100m (328ft) UTP run from a repeater out to the endstations.

Configuration Rules with Full Duplex

The Switch 3000 FX provides full duplex support for all its ports (including the optional Plug-in Module port, but not the Transceiver Module port). Full duplex allows frames to be transmitted and received simultaneously and, in effect, doubles the potential throughput of a link.

With full duplex, the Ethernet topology rules are the same, but the Fast Ethernet rules are:

- Maximum UTP cable length is 100m (328ft) over category 5 cable.
- A 2km (6562ft) fiber run is allowed for connecting switch-to-switch, or endstation-to-switch.

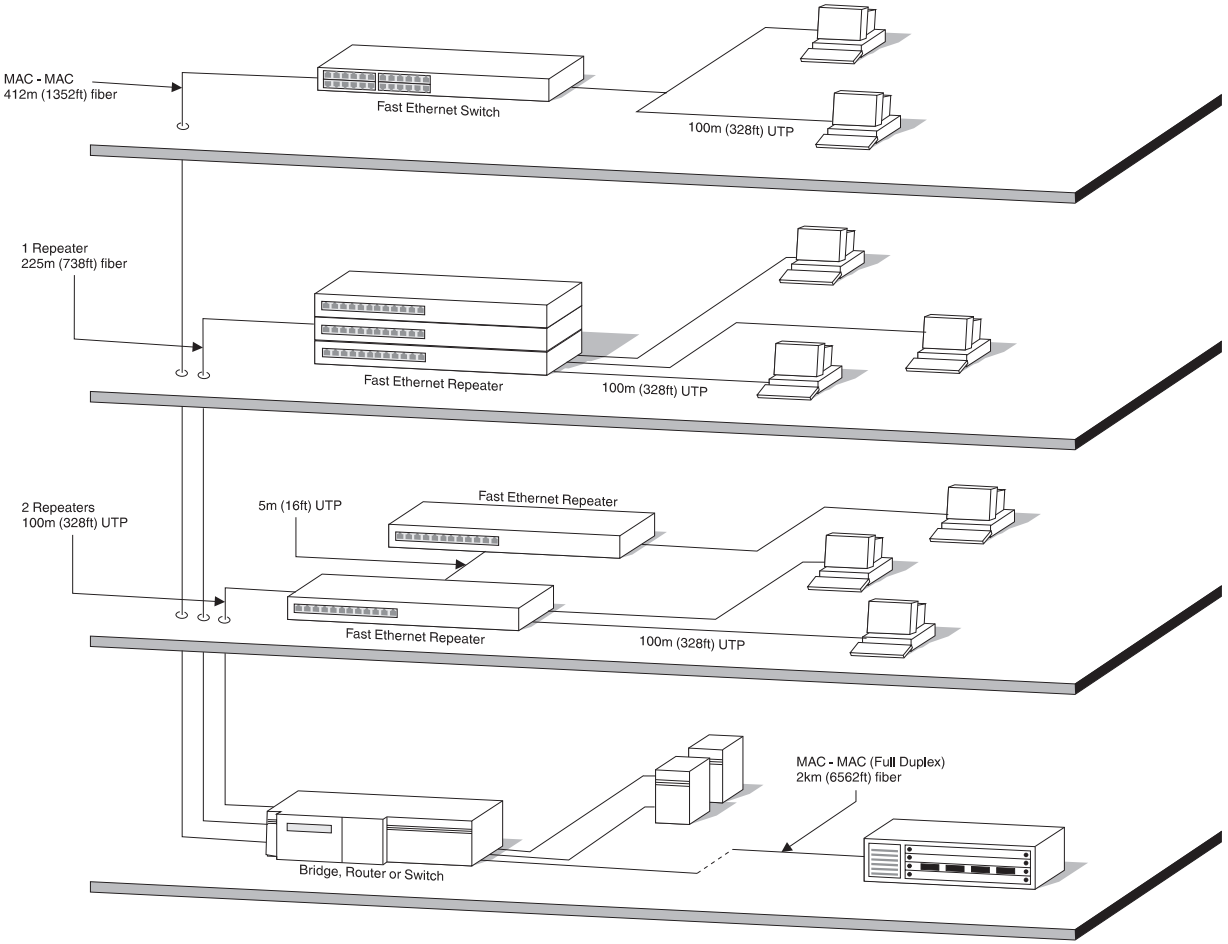


Figure 2-1 Fast Ethernet configuration rules

Installing the Switch 3000 FX

Rack Mounting

The Switch is 1.5U high and fits in most standard 19-inch racks.

CAUTION: *Disconnect all cables from the Switch before continuing. Remove all self adhesive pads from underside of the unit, if fitted.*

1 Place the unit the right way up on a hard flat surface, with the front facing towards you.

2 Locate a mounting bracket over the mounting holes on one side of the unit, as shown in Figure 2-2.

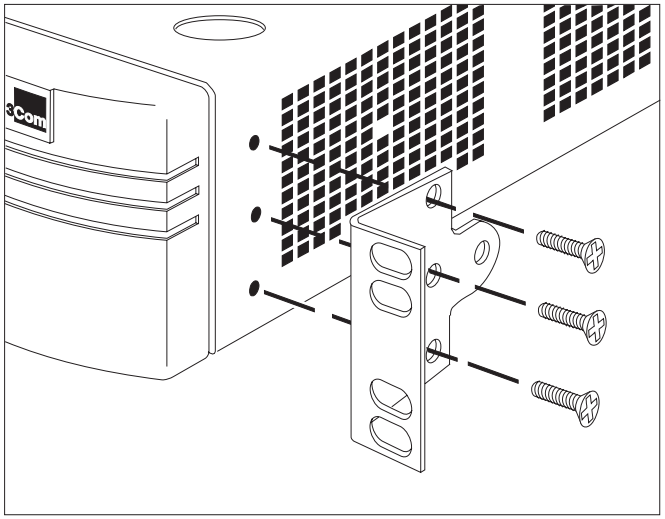


Figure 2-2 Fitting a bracket for rack mounting

3 Insert the three screws and fully tighten with a suitable screwdriver.

4 Repeat steps 2 and 3 for the other side of the unit.

5 Insert the unit into the 19-inch rack and secure with suitable screws (not provided). Ensure that ventilation holes are not obstructed.

6 Connect network cabling.

Stacking the Switch and Other Units

If the units are free standing, up to four units can be placed on top of one another. If mixing a variety of SuperStack II Switch and Hub units, the smaller units must be positioned at the top.

The Switch is supplied with four self-adhesive rubber pads. Apply the pads to the underside of the unit, sticking one in the marked area at each corner of the unit. Place the units on top of each other, ensuring that the pads of the upper unit line up with the recesses of the lower unit.

Wall Mounting

A single Switch can be wall-mounted.

CAUTION: *Disconnect any cables from the unit before continuing. Remove self-adhesive pads from the underside of the unit if they have been previously fitted.*

1. Place the Switch the right way up on a hard flat surface, with the front facing towards you.
2. Locate a mounting bracket over the mounting holes on one side of the unit, as shown in Figure 2-3.
3. Insert the two screws and tighten with a suitable screwdriver.
4. Repeat for the other side of the unit.
5. Ensure that the wall you are going to use is smooth, flat, dry and sturdy. Attach a piece of plywood, approximately 305mm x 510mm x 12mm (12in. x 20in. x 0.5in.) securely to the wall if necessary, and mount the Switch as follows:
   a. Position the base of the unit against the wall (or plywood) ensuring that the ventilation holes face sidewards. Mark on the wall the position of the screw holes in both wall brackets. Drill the four holes.
   b. Using suitable fixings and screws (not provided), attach the Switch unit securely to the wall or plywood.
   c. Connect network cabling.

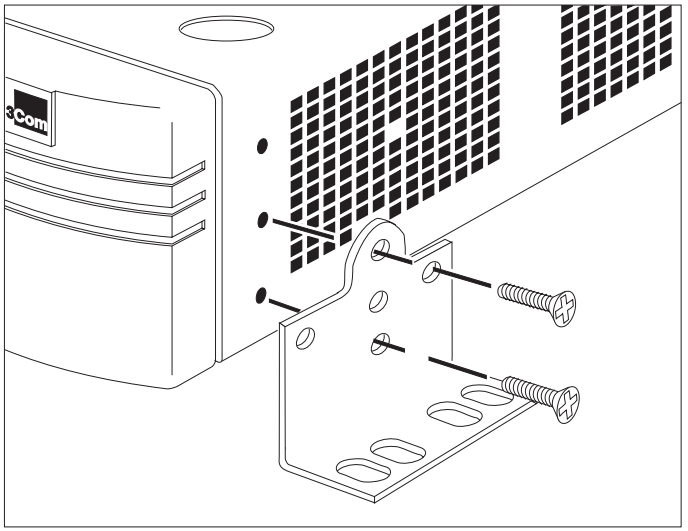


Figure 2-3 Fitting a bracket for wall mounting

Powering-Up the Switch

1 Connect the power cord to the IEC socket on the rear of the Switch, and to your mains socket.

The Switch has no ON/OFF switch; the only method of connecting or disconnecting mains power is through the power cord.

2 The Switch enters a Power On Self Test (POST). The time taken for the test to complete is dependent on the type of POST configured. (Refer to "Switch Management Setup" on page 3-9 for details of how to configure the type of POST.) For a new Switch that is being installed for the first time, power-up takes approximately 15 seconds.

3 Check the status LEDs to ensure the Switch is operating correctly (refer to "LEDs" on page 1-9).

Connecting a Redundant Power System (RPS)

You can connect a Redundant Power System (RPS) to the Switch.

At +5V, the current requirement for the Switch is 4.8A, including any Transceiver Module that might be fitted, but excluding a Plug-in Module. Check the documentation supplied with your Plug-in Module for power consumption figures.

For most configurations, you only need one SuperStack II RPS output, and this can be connected to either of the two sockets on the rear of the unit.

If the current consumption of the Switch plus any optional Plug-in Module exceeds the capability of the RPS (8.5A), you need a SuperStack II Advanced RPS with one Advanced RPS 100W Module.

If the RPS is used incorrectly, its Output Fault LED lights yellow.

You should check the documentation supplied with the RPS or Advanced RPS to see if the outputs can be used in parallel.

Connecting Equipment to the Console Port

The Switch console port settings are set to:

- 8 data bits
- no parity
- 1 stop bit

The terminal connected to the console port on the Switch must be configured with the same settings. This procedure is described in the documentation supplied with the terminal. If you have enabled auto-configuration for the Switch, the terminal's line speed (baud rate) is detected automatically.

Connection to the console port can be direct for local management, or through a modem for remote management. The maximum baud rate the auto-configuration detects is 19,200 baud.

Appropriate cables are available from your local supplier. If you need to make your own cables, pin-outs are detailed in Appendix D.

Connecting a VT100 Terminal

To connect a VT100 terminal directly to the console port on the Switch, you need a standard null modem cable:

1. Connect one end of the cable to the console port on the Switch, and the other to the console port on the VT100 terminal.
2. Ensure that your terminal is set to:
   - 8 data bits
   - no parity
   - 1 stop bit

   If auto-configuration is enabled for the Switch, the terminal's line speed (baud rate) is detected automatically.

Connecting a VT100 Terminal Emulator

1. Ensure that the workstation is running a suitable terminal emulation package. There are many available; contact your local supplier for further details.
2. If you are using a PC, you need a null modem cable with an appropriate connector. Connect one end of the cable to the workstation, and the other end to the console port on the Switch.
3. Ensure that your workstation is set to:
   - 8 data bits
   - no parity
   - 1 stop bit

   If auto-configuration is enabled on the Switch, the workstation's line speed (baud rate) is detected automatically.

Connecting a Workstation Running SLIP

You can communicate with the Switch via the console port from a workstation running SLIP (Serial Line Internet Protocol). In this way, you can perform out-of-band management using Telnet or SNMP.

Cables required for this connection depend on the type of workstation you are using. You must configure the workstation to run SLIP. Refer to the documentation supplied with the workstation for more details.

You must configure the console port of the Switch to accept SLIP and set up the SLIP parameters (address and subnet mask). Refer to "Switch Management Setup" on page 3-9.

You may need a 5-wire cable when running SLIP. Two of the wires are required for Flow Control.

3 SETTING UP FOR MANAGEMENT

Methods of Managing the Switch

You can manage the Switch 3000 FX in four ways:

- Using the VT100 interface by connecting a VT100 terminal (or workstation with terminal emulation software) to the Switch 3000 FX console port.
- Using the VT100 interface over a TCP/IP network using a workstation running VT100 terminal emulation and Telnet.
- Using the VT100 interface by connecting a workstation running SLIP to the Switch 3000 FX console port.
- Using an SNMP Network Manager over a network running either the IP or IPX protocol. Each Network Manager provides its own user interface to the management facilities.

Using the VT100 Management Interface

The menu-driven user interface built into the Switch is known as the *VT100* or *local management* interface. The VT100 management interface gives a forms-based structure with pre-defined security levels, enabling access to be restricted to particular users.

The Switch can support up to four management user sessions concurrently (for example, one console port and three Telnet connections).

You can establish VT100 management communication with the Switch through two different interfaces:

- **Via the Console Port** — You can access the local management interface using a VT100 terminal, or PC using suitable terminal emulation software. The terminal can be connected directly to the Switch, or via a modem. You can also connect a management workstation running SLIP to the console port, which allows you to use out-of-band Telnet. The workstation can be connected directly or remotely, via a modem. This method provides a way of managing the Switch in situations where the LAN is not providing a reliable service, or where the Network Manager does not have direct LAN connectivity or when a Network Manager does not support SNMP.
- **Via a Network Connection** — The local management facility is also accessible via Telnet over a network running the TCP/IP protocol. The management available through Telnet is exactly the same as that of a locally connected terminal. The Telnet application requires a VT100 terminal or PC with VT100 emulation software.

Using Telnet

Any Telnet facility that emulates a VT100 terminal should be able to communicate with the Switch over a TCP/IP network. Up to three active Telnet sessions can access the Switch concurrently. If a connection to a Telnet session is lost inadvertently, the connection is closed by the Switch after 2–3 minutes of inactivity.

Before you can start a Telnet session you must set up the IP parameters described in "Switch Management Setup" on page 3-9.

To open the Telnet session, you must specify the IP address of the device that you want to manage. Check the user manual supplied with the Telnet facility if you are unsure how to do this.

Once the connection is established, the main banner of the VT100 management interface is displayed and you can log on.

Managing Over The Network

Any Network Manager running the Simple Network Management Protocol (SNMP) can manage the Switch 3000 FX, provided the MIB (Management Information Base) is installed correctly on the management workstation.

Each Network Manager provides its own user interface to the management facilities. 3Com's Transcend® range of Network Managers all have facilities for managing the Switch 3000 FX.

The Switch 3000 FX supports SNMP over both IP and IPX protocols.

IP Addresses

If you are uncertain about IP addresses that may be assigned to your devices, contact your network administrator first.

To operate correctly, each device on your network must have a unique IP address. IP addresses have the format n.n.n.n where n is a decimal number between 0 and 255. An example IP address is: 191.128.40.120

The IP address can be split into two parts:

- The first part (191.128 in the example) identifies the network on which the device resides.
- The second part (40.120 in the example) identifies the device within the network.

If your network is internal to your organization only, you may use any arbitrary IP address. We suggest you use addresses in the series 191.100.X.Y, where X and Y are numbers between 1 and 254. Use 191.101.X.Y for the SLIP address.

If your network has a connection to the external IP network, you will need to apply for a registered IP address. This system ensures that every IP address used is unique; if you do not have a registered IP address, you may be using an identical address to someone else and your network will not operate correctly.

Obtaining a Registered IP Address

InterNIC Registration Services is the organization responsible for supplying registered IP addresses. The following contact information is correct at the time of publication:

Network Solutions
Attn: InterNIC Registration Service
505, Huntmar Park Drive
Herndon
VA 20170
U.S.A.

Telephone: (1) (703) 742 4777

If you have access to the Internet, you can find further information about InterNIC by entering the following URL into your web browser:

`http://www.internic.net`

Navigating the VT100 Screens

Screen Conventions

To differentiate types of information, the VT100 screens use the following conventions:

Type of information	Shown on screen as...	Description
Choice Field	♦text♦	Text enclosed with markers is a list from which you can select one option only. Press the spacebar to cycle through the options. Press [Down Arrow] or [Return] to move to the next field.
Entry Field	[text]	Text enclosed in square brackets on the screen is a *text entry* field. A text entry field allows you to enter text, numeric data or hexadecimal data from the keyboard. Password fields are hidden, which means that the text you type is not shown on the screen. In some cases a text entry field has a default entry. If you wish to replace the default, simply enter a new value for this field; the default entry is erased. Press [Down Arrow] or [Return] to move to the next field.
Button	OK	Text for a button is always shown in uppercase letters. A button carries out an action. For example, OK or CANCEL. To operate a button move the cursor to the button and press [Return].
List Box	monitor manager security	A list box allows you to select one or more items from a list. There are several keys that allow you to use a list box: ■ [Return] moves the cursor to the next field and actions your selections. ■ The spacebar toggles through the options in a choice field or selects and deselects an entry in the list box. List box selections will be highlighted. ■ [Down Arrow] moves item by item down the list box until it reaches the end of the list. At the end of the list it moves the cursor to the next field. ■ [Ctrl] + [U] moves the cursor one page up the list box. ■ [Ctrl] + [D] moves the cursor one page down the list box.

Keyboard Shortcuts

There are several special characters or combinations of characters that allow you to make shortcuts:

[Tab] allows you to move from one field to the next, on any screen without making any changes.

[Return] moves you to the next field on a form after you have made changes to the data in a field.

[Left Arrow] moves you to the previous field on the screen or the next character in an editable field.

[Right Arrow] moves you to the next field on the screen or the previous character in an editable field.

[Ctrl] + [R] refreshes the screen.

[Ctrl] + [B] moves the cursor to the next button.

[Ctrl] + [P] aborts the current screen and returns you to the previous screen.

[Ctrl] + [N] actions the inputs for the current screen and moves to the next screen.

[Ctrl] + [K] displays a list of the available key strokes.

Correcting Text Entry

Use [Delete] on a VT100 terminal or [Backspace] on a PC. This moves the cursor one space to the left and deletes a character.

If you are using Telnet or a terminal emulation program you may find that some of the Control keys do not operate or that they activate other functions. Check carefully in the manual accompanying your Telnet or terminal emulation software before using the Control keys.

Setting up the Switch for Management

The following sections describe how to get started if you want to use an SNMP Network Manager to manage the Switch. It assumes you are already familiar with SNMP management. If not, we recommend the following publication:

"The Simple Book" by Marshall T. Rose
ISBN 0-13-812611-9
Published by Prentice Hall

- If you are using IP and you have a BOOTP server set up correctly on your network, the IP address for the Switch is detected automatically and you can start managing the Switch without any further configuration.
- If you are using the IPX protocol, the Switch is allocated an IPX address automatically. You can start the SNMP Network Manager and begin managing the Switch.
- If you are using IP without a BOOTP server, you must enter the IP address of the Switch before the SNMP Network Manager can communicate with the device. To do this, take the following steps:

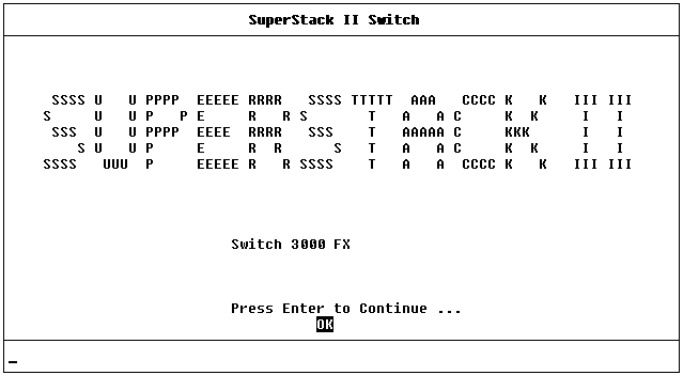


Figure 3-1 Main Banner

1. At your terminal, press [Return] one or more times until the Switch 3000 FX Main Banner is displayed (shown in Figure 3-1). The console port detects the line-speed (baud rate) from these keystroke and defaults to:
   - auto-baud
   - 8 data bits
   - no parity
   - 1 stop bit

   Data bits, parity, and stop bit values cannot be changed.
2. At the Main Banner, press [Return] to display the Logon screen.

Logging On

At the Logon screen displayed in Figure 3-2, enter your user name and password (note that they are both case-sensitive):

- If you have been assigned a user name and password, enter those details.
- If you are logging on for the first time (after installation or initialization), use a default user name and password to match your access requirements. The defaults are shown in Table 3-1. If you are setting up the Switch for management, we suggest that you log on first as *admin*.

Table 3-1 Default Users

User Name	Default Password	Access Level
monitor	monitor	monitor — this user can view, but not change all manageable parameters
manager	manager	manager — this user can access and change the operational parameters but not special/security features
security	security	security — this user can access and change all manageable parameters
admin	(no password)	security — this user can access and change all manageable parameters

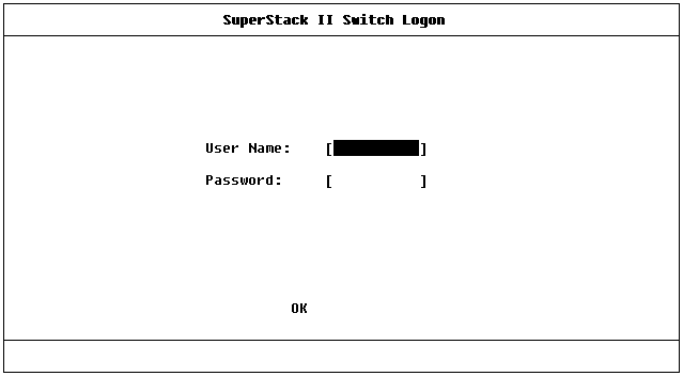


Figure 3-2 Logon screen

After Logging On

When you have successfully logged on to the Switch, the Main Menu screen is displayed, as shown in Figure 3-3. From here, you can select the options needed to manage the unit. Refer to the screen map on page 4-1.

If you have installed an ATM OC-3c Module into the Switch, the Main Menu screen contains an ATM CONFIGURATION option. Refer to the "SuperStack II Switch ATM OC-3c Module User Guide" for more information.

Access to options depends on the access level you have been assigned. Access rights to the VT100 screens for the Switch are listed in Appendix B.

If you are a user with *security* access level, and are using the management facility for the first time, we suggest that you:

- Assign a new password for your user, using the Edit User screen, as described in "Editing User Details" on page 4-5.
- Log on as each of the other default users, and change their passwords using the Edit User screen.
- Create any new users, in addition to the default ones. To do this, you assign each a user name, password, and security level, as described in "Creating a New User" on page 4-3.

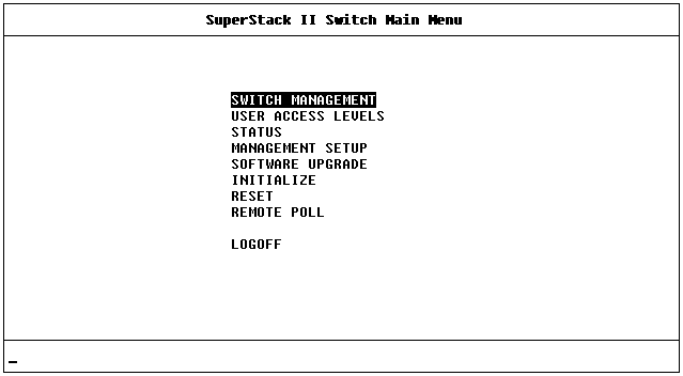


Figure 3-3 Main Menu screen

Switch Management Setup

The Management Setup screen allows you to configure IP, IPX, and SLIP parameters for the Switch. This screen also allows you to display screens for setting up the console port and traps.

To access the Setup screen, from the Switch Main Menu screen, select the MANAGEMENT SETUP option. The Setup screen is displayed, as shown in Figure 3-4.

If you change some of the following parameters, the Switch must be reset for the change to take effect. Reset the Switch by selecting OK and pressing the Reset button on the rear of the unit. Refer to "Unit Overview — Rear" on page 1-10.

The screen shows the following:

MAC Address This read-only field shows the MAC address of the Switch unit, which is required for management.

Power On Self Test Type *Normal / Extended* This field allows you to determine the type of self-test that the Switch carries out when it is powered-up. If the field is set to *Normal,* the Switch performs a Fast Boot — a basic confidence check lasting approximately 15 seconds. When the Switch performs a Fast Boot, it carries out the following tests:

- Checksum test of boot and system areas of Flash memory
- System memory tests
- MAC address verification test

```
                    SuperStack II Switch Management Setup

MAC Address:                 08004E0B99A5

Power On Self Test Type:   ♦Normal  ♦

Device IP Address: [191.1.1.50     ]    SLIP Address:    [192.101.1.1    ]
Device SubNet Mask:[255.255.255.0  ]    SLIP SubNet Mask:[255.255.255.0  ]
Default Router:    [191.1.1.20     ]
BOOTP Select:      ♦Enabled ♦

IPX Network  Node            Status    Data Link Protocol
[00356501] : 08004e0b99a5  ♦Enabled ♦ Ethernet_802.3
[00356502] : 08004e0b99a5  ♦Enabled ♦ Ethernet_802.2
[00356503] : 08004e0b99a5  ♦Enabled ♦ Ethernet_II
[00000000] : 08004e0b99a5  ♦Enabled ♦ Ethernet_SNAP


                OK    SETUP TRAPS   CONSOLE PORT   CANCEL

-
```

Figure 3-4 Management Setup screen

- System timer test
- CAM (Contents Addressable Memory) tests
- Console port tests
- Internal packet forwarding tests
- ASIC (Application Specific Integrated Circuit) tests
- ASIC memory tests
- Switch–Plug-in Module interface test
- Plug-in Module packet forwarding tests
- Plug-in Module ASIC tests
- Plug-in Module ASIC memory tests

If the field is set to *Extended*, the Switch performs an Extended test which may take up to 2 minutes to complete. When the Switch performs an Extended test, it carries out more extensive system memory tests and ASIC memory tests in addition to the Fast Boot tests. The default setting for the field is *Normal*.

If you suspect that there is a problem with the Switch that has not been detected by the Normal tests, set this field to Extended and reset the Switch (refer to "Resetting the Switch 3000 FX" on page 4-26).

If you set the Switch to perform an Extended test, the Switch must be disconnected from the rest of your network when it is powered-up. The Switch fails an Extended test if it receives any network traffic during the test.

Device IP Address If you are using IP, a unique IP address must be specified in this field. If you do not know the IP address of the Switch, consult your network administrator. You must reset the Switch after changing this parameter.

Device SubNet Mask If you are using IP, enter a suitable network mask. For a Class B IP address, 255.255.0.0 is suitable. For more information, consult your network administrator. You must reset the Switch after changing this parameter.

Default Router If a default router exists on your network, enter the IP address of the router. You must reset the Switch after changing this parameter.

BOOTP Select *Enabled / Disabled* If BOOTP is enabled and you have a BOOTP server on your network, an IP address is automatically mapped to the Switch when it is first powered-up. In addition to mapping an IP address, BOOTP can also assign the subnet mask and default router. Using a BOOTP server avoids having to configure devices individually.

SLIP Address If you are using SLIP, enter an address that has a network part different to the network address of the Switch. For more information, consult your network administrator. You must reset the Switch after changing this parameter.

SLIP SubNet Mask Enter a suitable SubNet Mask. For a Class B address, 255.255.0.0 is suitable. For more information, consult your network administrator. You must reset the Switch after changing this parameter.

There are four entries under the following four fields; one for each data link layer protocol that can be used by IPX:

IPX Network This read-only field shows the address of the network for this protocol. This address is learned automatically from the local IPX router or Netware file server, and you do not need to change it.

Node This read-only field shows the node address of the Switch which is learned automatically.

Status *Enabled / Disabled* If this field is set to Enabled, you have access to the medium-access protocol. Set this field to Disabled if you wish to prevent access for security reasons.

Data Link Protocol This read-only field shows the name of the IPX data link layer protocol.

SETUP TRAPS Select this button to display the setup screen for trap parameters. Trap Setup is described in "Setting Up Traps" on page 4-23.

CONSOLE PORT Select this button to display the setup screen for console port parameters. Console port setup is described in "Setting Up the Console Port" on page 4-24.

Logging Off

If you have finished using the VT100 management interface, select the LOGOFF option from the bottom of the main menu. If you accessed the VT100 management interface using a Telnet session or modem connection, the connection is closed automatically.

Auto Logout

There is a built-in security timeout on the VT100 interface. If you do not press any keys for 3 minutes, the management facility warns you that the inactivity timer is about to expire. If you do not press a key within 10 seconds, the timer expires and the screen is locked; any displayed statistics continue to be updated. When you next press any key, the display changes to the Auto Logout screen.

The Auto Logout screen (shown in Figure 3-5) requests you to enter your password again. If the password is correctly entered, the screen that was active when the timer expired is displayed. If you make a mistake entering your password, you are returned to the Logon screen.

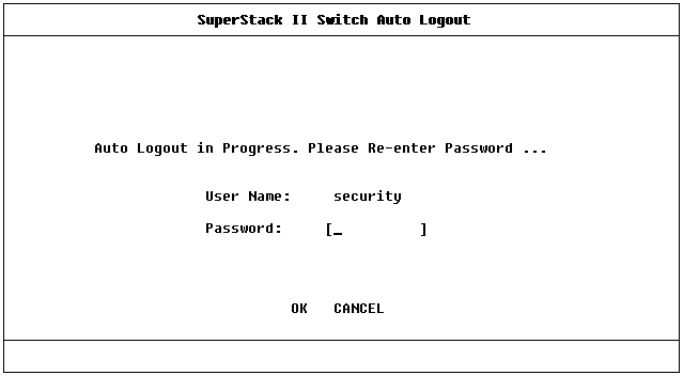

SuperStack II Switch Auto Logout
Auto Logout in Progress. Please Re-enter Password ...
User Name: security
Password: [_]
OK CANCEL

Figure 3-5 Auto Logout screen

4 MANAGING THE SWITCH 3000 FX

Chapters 4, 5 and 6 describe all management facilities for the Switch. While following steps in these chapters, you may find the screen map below useful:

If an ATM OC-3c Module is installed in the Switch, extra screens are available. Refer to the "SuperStack® II Switch ATM OC-3c Module User Guide" for more information.

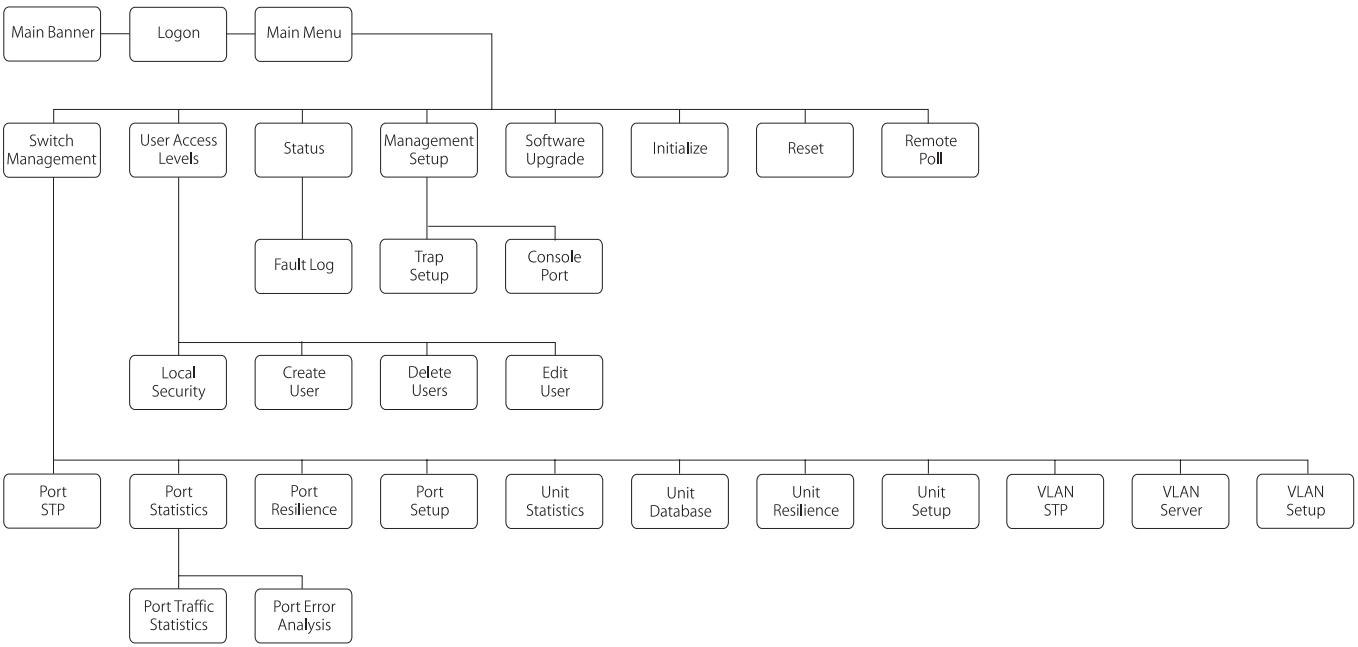


Figure 4-1 Screen map

Setting Up Users

From the Main Menu, select USER ACCESS LEVELS. The User Access Levels screen is displayed as shown in Figure 4-2.

From this screen you can access:

- **LOCAL SECURITY screen** — This allows you to set up access levels for users on the Switch.
- **CREATE USER screen** — This allows you to create up to 10 users in addition to the default users set up on the Switch.
- **DELETE USERS screen** — This allows you to delete users from the Switch. The default users cannot be deleted.
- **EDIT USER screen** — This allows you to change your own password and community string. You cannot change details for other users.

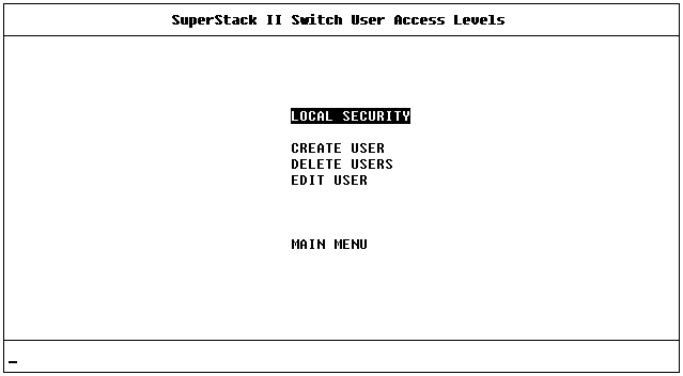


Figure 4-2 User Access Levels menu

Creating a New User

These steps assume the User Access Levels screen is displayed.

1 Select the CREATE USER option. The Create User screen is displayed, as shown in Figure 4-3.

2 Fill in the fields and assign an access level for the new user.

3 When the form is complete, select OK.

The Create User screen shows the following fields:

User Name Type in the name of this new user. The name can consist of up to 10 characters and is case-sensitive.

Password Type in the password for this new user. The password can consist of up to 10 characters and is case-sensitive. For security reasons, the password is not displayed on screen.

Access Level Assign an access level for this new user, as follows:

- *monitor* — access to view, but not change, a subset of the manageable parameters of the Switch
- *secure monitor* — as *monitor*
- *manager* — access to all the manageable parameters of the Switch, except security features
- *specialist* — as *manager*
- *security* — access to all manageable parameters of the Switch

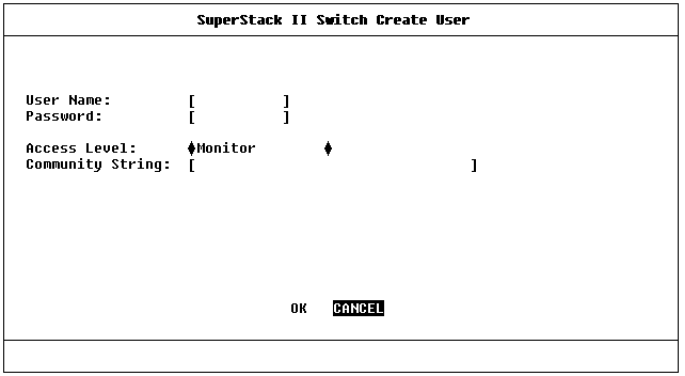


Figure 4-3 Create User screen

Community String By default, a community string identical to the user name is generated. You can change this to any text string of 32 characters or less. The community string is only needed for SNMP access. If you are using a remote SNMP Network Manager, the community string specified in the Network Manager's database must be the same as that for the device.

If you enter a community string that is greater than 32 characters, it is truncated to 32 characters.

Deleting a User

These steps assume the User Access Levels screen is displayed.

1. Select the DELETE USERS option. The Delete Users screen is displayed, as shown in Figure 4-4.
2. Use the spacebar to highlight the user that you want to delete. Note that you cannot delete default users or the current user (that is, yourself).
3. Select DELETE USERS.

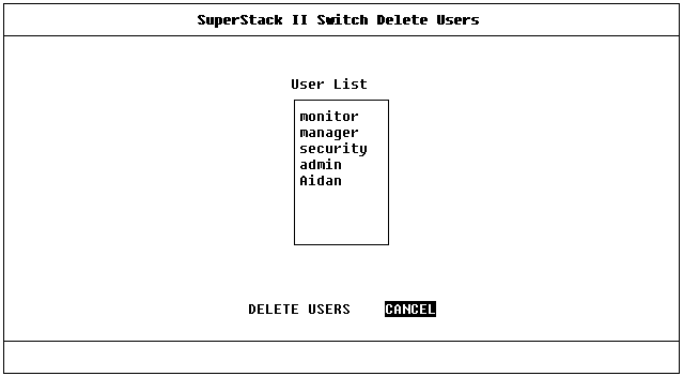


Figure 4-4 Delete Users screen

Editing User Details

These steps assume the User Access Levels screen is displayed.

1 Select the EDIT USER option. The Edit User screen is displayed, as shown in Figure 4-5.

2 Fill in the fields as required.

3 When you have completed the changes, select OK.

The Edit User screen shows the following fields:

User Name This read-only field shows the name of the user. This field cannot be changed; if you need to change the user name, you must delete this user and create a new one.

Old Password To change the user's password, you need to enter the current password in this field.

New Password This field allows you to enter a new password for the user.

Confirm Password Re-enter the new password into this field.

Community String This field allows you to enter a community string for the user.

If you forget your password while logged out of the Switch VT100 interface, contact your local technical support representative who will advise on your next course of action.

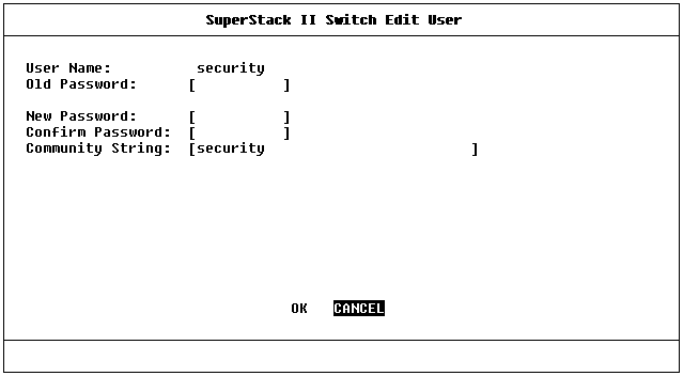


Figure 4-5 Edit User screen

Assigning Local Security

The Local Security screen shows a matrix of options for access method (Console Port, Remote Telnet, Community-SNMP) and access level.

These steps assume the User Access Levels screen is displayed.

1 Select the LOCAL SECURITY option. The Local Security screen is displayed, as shown in Figure 4-6.

2 Fill in the fields as required.

3 When you have filled in the form, select OK.

The access options are:

Console Port *Enabled* / *Disabled* To prevent access to the management facilities via the console port, disable access to the facility for each access level. Console Port access for *Security* is enabled and cannot be changed. This prevents accidental disabling of all access levels from management.

Remote Telnet *Enabled* / *Disabled* Telnet is an insecure protocol. You may want to disable all access to the management facilities via Telnet if there is important or sensitive data on your network.

Community-SNMP *Enabled* / *Disabled* The Switch can be managed via SNMP using a remote Network Manager. Community SNMP does have some simple security features, but it is an insecure protocol. You may want to disable all access to the management facilities if there is important or sensitive data on your network.

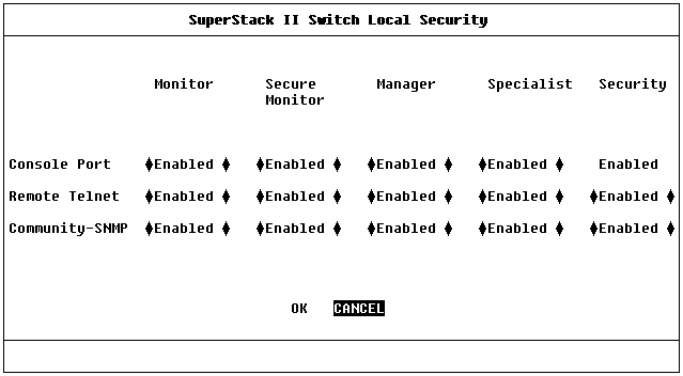


Figure 4-6 Local Security screen

Choosing a Switch Management Level

The Switch Management screen allows you to:

- Choose between managing a port, the unit, or a VLAN
- Display screens for setting up the Switch
- Display a screen for managing the Switch Database
- Display screens for managing resilient links
- Display screens for managing STP
- Display screens showing statistics

From the Main Menu, select SWITCH MANAGEMENT. The Switch Management screen is displayed, as shown in Figure 4-7.

Management Level *Port / Unit / VLAN* If you choose *Port*, the screen is displayed similar to Figure 4-7, and all options at the foot of the screen relate to an individual port. If you choose *Unit*, the screen is displayed similar to Figure 4-8, and all options relate to the Switch unit. If you choose *VLAN*, the screen is displayed similar to Figure 4-9, and all options relate to VLANs.

Port ID *1 / 2 / 3 ... 6 / 7 / 8* If you choose to manage the Switch at port level, enter the particular port number into this field before selecting the next screen. Ports 1–5 are the 100BASE-FX ports, port 6 is the Transceiver Module, port 7 is the Plug-in Module at the rear of the unit, and port 8 is the 100BASE-TX port.

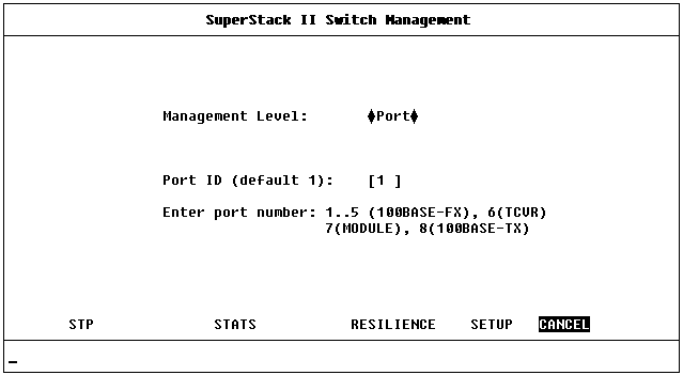


Figure 4-7 Switch Management screen for Port level

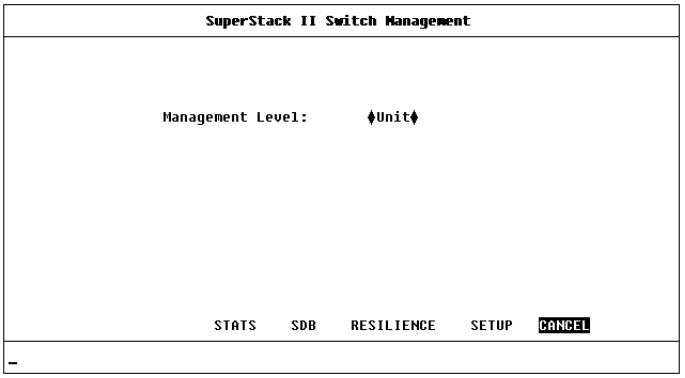


Figure 4-8 Switch Management screen for Unit level

STP Use this button to display screens for managing Spanning Tree Protocol (STP) information for the level of management you have chosen (port or VLAN). Refer to "Spanning Tree Protocol" on page 5-12.

STP is not supported over Asynchronous Transfer Mode (ATM). Consequently, if you specify that you want to manage the Plug-in Module port and the Switch has an ATM OC-3c Module installed, the STP button is not displayed.

SERVER Use this button to display the VLAN Server screen, used for entering the IP address and community string of a VLAN server. For more information about VLAN servers, refer to "Virtual LANs (VLANs)" on page 5-1.

STATS Use this button to display statistics screens for the level of management you have chosen (port or unit). Refer to Chapter 6.

SDB Use this button to display the Unit Database View screen, which is used to manage the Switch Database. Refer to "The Database View" on page 4-16.

RESILIENCE Use this button to display resilient link management screens for the level of management you have chosen (port or unit). Refer to "Setting Up Resilient Links" on page 4-18.

You cannot set up resilient links if the Switch uses Spanning Tree (STP). Consequently, the RESILIENCE button is not displayed if STP is enabled.

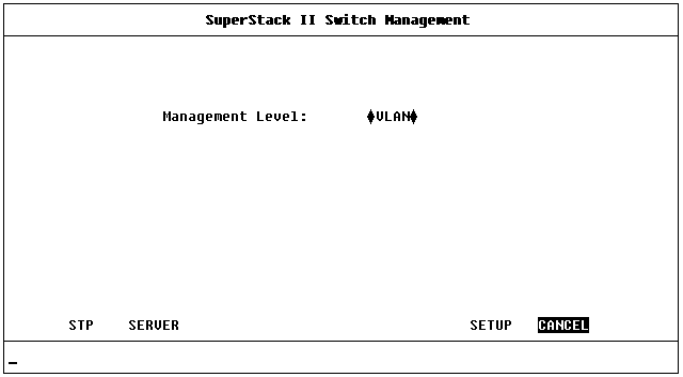


Figure 4-9 Switch Management screen for VLAN level

SETUP Use this button to display setup screens for the level of management you have chosen (port, unit or VLAN). For information about the Port Setup and Unit Setup screens, refer to "Setting Up the Switch Ports" and "Setting Up the Switch Unit" in this chapter. For information about the VLAN Setup screen, refer to "Setting Up VLANs on the Switch" on page 5-8.

Setting Up the Switch Unit

With the Switch Management screen displayed, choose the management level *Unit*, then select the SETUP button.

The Unit Setup screen is displayed as shown in Figure 4-10. The screen shows the following:

Unit Name This read-only field shows the type of device.

sysName This field takes its name from the MIB II System Group object. You can edit the first 30 characters of this field to make the name more meaningful. This name is displayed on the Main Banner when you first access the VT100 screens, and is also accessible to an SNMP Network Manager.

PACE *Enable / Disable* This field allows you to enable or disable PACE (Priority Access Control Enabled) for all ports on the Switch. PACE allows multimedia traffic to be carried over standard Ethernet and Fast Ethernet LANs by providing two features:

- *Implicit Class of Service* — When multimedia traffic is transmitted, it is given a higher priority than other data and is therefore forwarded ahead of other data when it arrives at the Switch. The Implicit Class of Service feature minimizes latency through the Switch and protects the quality of multimedia traffic.

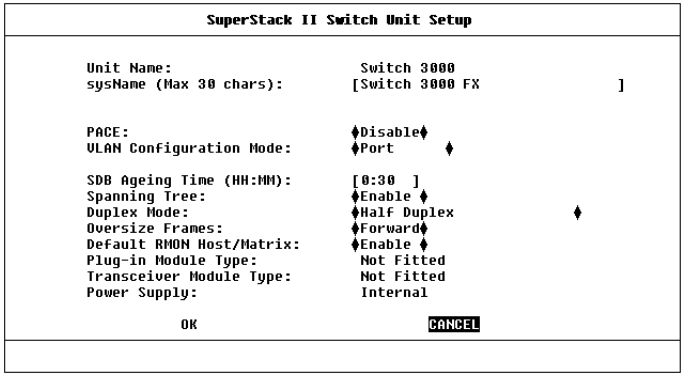

SuperStack II Switch Unit Setup
Unit Name: Switch 3000
sysName (Max 30 chars): [Switch 3000 FX]
PACE: ♦Disable♦
VLAN Configuration Mode: ♦Port ♦
SDB Ageing Time (HH:MM): [0:30]
Spanning Tree: ♦Enable ♦
Duplex Mode: ♦Half Duplex ♦
Oversize Frames: ♦Forward♦
Default RMON Host/Matrix: ♦Enable ♦
Plug-in Module Type: Not Fitted
Transceiver Module Type: Not Fitted
Power Supply: Internal
OK
CANCEL

Figure 4-10 Unit Setup screen

- *Interactive Access* — When two-way multimedia traffic passes over an Ethernet network, interference can occur because access to the bandwidth is unequally allocated to traffic in one direction. The Interactive Access feature allocates the available bandwidth equally in both directions, therefore increasing the quality of the traffic.

Interactive Access should only be enabled on ports that connect to a single endstation, switch, bridge, or router. You should disable Interactive Access on a port if it is connected to a repeater. Also, Interactive Access should be enabled at only one end of a link.

For more information about disabling Interactive Access for a port, refer to "Setting Up the Switch Ports" on page 4-11.

VLAN Configuration Mode *Port / AutoSelect* This field allows you to specify how ports on the Switch are placed in VLANs:

- *Port* — The ports use Port VLAN Mode, which means that they are manually placed in the required VLAN. This is the default mode.
- *AutoSelect* — The ports use AutoSelect VLAN Mode, which means that they are automatically placed in the required VLAN by referring to a VLAN Server database in 3Com's Transcend® Enterprise Manager software.

For more information, refer to "Using AutoSelect VLAN Mode" on page 5-4.

SDB Ageing Time This field allows you to specify the ageing time (hours:minutes) for all non-permanent entries in the Switch Database of the unit. You can set an ageing time in the range 0 minutes to 277 hours, with a default of 30 minutes. If you enter 0:00, ageing is turned off. For more information about ageing times, refer to "Setting Up the Switch Database (SDB)" on page 4-15.

Spanning Tree *Enable / Disable* This field allows you to enable or disable the Spanning Tree Protocol (STP) on the Switch. For more information about STP, refer to "Spanning Tree Protocol"on page 5-12.

Duplex Mode *Half Duplex / Full Duplex on 100M Ports* This field allows you to set the duplex mode for ports that have Unit Default specified in the Duplex Mode field of the Port Setup screen. The default setting is Half Duplex. For more information about Duplex Mode, refer to "Setting Up the Switch Ports" on page 4-11.

Oversize Frames *Forward / Discard* This field allows you to specify whether the Switch forwards encapsulated Token Ring frames from 3Com's Token Ring products. Set this field to Forward if the Switch is connected to 3Com products which support Token Ring encapsulation (for example, the SuperStack II Switch 2000); otherwise set the field to Discard.

Default RMON Host/Matrix *Enable / Disable* This field allows you to specify whether Hosts and Matrix RMON sessions are defined on the Default VLAN. The default setting for this field is Disable. For more information about RMON sessions, refer to "RMON" on page 5-22.

Plug-in Module Type This read-only field displays the type of Plug-in Module fitted to the rear of the unit, or displays *Not Fitted*.

Transceiver Module Type This read-only field displays the type of Transceiver Module fitted to the rear of the unit, or displays *Not Fitted*.

Power Supply *Internal / External* This read-only field displays *External* if the Switch is receiving power from a Redundant Power System. In all other cases, this field displays *Internal*.

Setting Up the Switch Ports

With the Switch Management screen displayed, choose the management level *Port*. Choose the appropriate port, then select the SETUP button.

The Port Setup screen is displayed, as shown in Figure 4-11.

If the port is an ATM OC-3c Module port, the ATM Port Setup screen is displayed. For more information, refer to the "SuperStack II Switch ATM OC-3c Module User Guide".

The screen shows the following:

Port ID This read-only field shows the ID of the port you have chosen to setup.

Media Type This read-only field shows the media type of the link connected to this port.

Port Speed *100Mbps HD / 100Mbps FD / 10Mbps HD* This read-only field shows the speed and duplex mode of the link. HD indicates half duplex, and FD indicates full duplex.

Port State *Enable / Disable* This field allows you to enable or disable the port. To prevent unauthorized access, we recommend that you disable any unused ports.

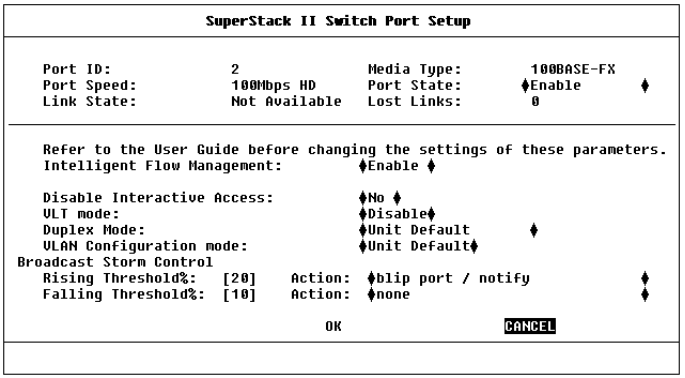

SuperStack II Switch Port Setup
Port ID: 2
Media Type: 100BASE-FX
Port Speed: 100Mbps HD
Port State: Enable
Link State: Not Available
Lost Links: 0
Refer to the User Guide before changing the settings of these parameters.
Intelligent Flow Management: Enable
Disable Interactive Access: No
VLT mode: Disable
Duplex Mode: Unit Default
VLAN Configuration mode: Unit Default
Broadcast Storm Control
Rising Threshold%: [20] Action: blip port / notify
Falling Threshold%: [10] Action: none
OK
CANCEL

Figure 4-11 Port Setup screen

Link State *Present / Not Available* This read-only field shows the state of the link:

- *Present* — The port is operating normally.
- *Not Available* — The link has been lost.

Lost Links This read-only field shows the number of times the link has been lost since the Switch was last reset. If the number in this field is not zero, you should check your cables and replace any that may be damaged.

If the port is directly connected to an endstation, the Lost Links counter increments each time the endstation goes through a power-off/on cycle.

Intelligent Flow Management *Enable / Disable* This field allows you to enable or disable Intelligent Flow Management (IFM). IFM minimizes packet loss which can occur with conventional switches.

IFM should be disabled if the port is connected to a repeated segment where the traffic is mainly local to that segment.

IFM is not available on a port that has full duplex enabled:

- *If the Duplex Mode field in this screen is set to Full Duplex, the Intelligent Flow Management field is not displayed*
- *In all other cases where the port has full duplex enabled, IFM has no effect*

Disable Interactive Access *Yes / No* This field allows you to disable the Interactive Access feature of PACE (Priority Access Control Enabled) on the current port. You should disable Interactive Access on a port if:

- The port is connected to a repeater
- The port is connected to a device with Interactive Access enabled

For more information about the Interactive Access feature, refer to "Setting Up the Switch Unit" on page 4-9.

VLT Mode *Enable / Disable* This field allows you to specify whether the port is a Virtual Lan Trunk (VLT) port. A Virtual LAN Trunk (or VLT) is a Switch-to-Switch link which carries traffic for all the VLANs on each Switch. To create a VLT, the ports on both ends of the link must be VLT ports.

For more information about VLTs, refer to "VLANs and the Switch 3000 FX" on page 5-3.

If the port uses AutoSelect VLAN Mode (refer to the VLAN Configuration Mode field), you cannot specify that the port is a VLT port.

Duplex Mode *Half Duplex / Full Duplex / Unit Default* This field allows you specify to the Duplex Mode of the port:

- *Full Duplex* — Full duplex allows frames to be transmitted and received simultaneously and, in effect, doubles the potential throughput of a link. In addition, full duplex also supports 100BASE-FX cable runs of up to 2km.

  You should only enable full duplex on a point-to point-link between the Switch and another device with full duplex support.
- *Half Duplex* — You should use half duplex if the port connects to a shared Ethernet or Fast Ethernet LAN segment, or if the device at the other end of a point-to-point link does not support full duplex.
- *Unit Default* — The Duplex Mode of the port is defined by the Duplex Mode field in the Unit Setup screen. This is the default setting.

Full duplex is not supported on the Transceiver Module port.

VLAN Configuration Mode *Port / AutoSelect / Unit Default* This field allows you to specify how the port is placed in a VLAN:

- *Port* — The port uses Port VLAN Mode, which means that the port is manually placed in the required VLAN.
- *AutoSelect* — The port uses AutoSelect VLAN Mode, which means that the port is automatically placed in the required VLAN by referring to a VLAN Server database in 3Com's Transcend Enterprise Manager software.
- *Unit Default* — The port uses Port VLAN Mode or AutoSelect VLAN Mode depending on the contents of the VLAN Configuration Mode field in the Unit Setup screen. This is the default setting.

For more information, refer to "Using AutoSelect VLAN Mode" on page 5-4.

Broadcast Storm Control The Switch automatically creates an alarm on each of its ports in order to monitor the level of broadcast traffic on each port. The Broadcast Storm Control fields allow you to specify thresholds for the level of broadcast traffic on a port, and specify an action to take place if the threshold is exceeded.

Rising Threshold% This field allows you to specify the percentage of broadcast traffic on the current port which triggers the alarm for the port. The default is 20%.

Falling Threshold% This field allows you to specify the percentage of broadcast traffic on the current port required to reset the alarm for the port. The falling threshold prevents the rising threshold events being triggered continuously. The default is 10%.

Rising Action *none / event / disable port / disable port/notify / blip / blip port/notify* Use this field to specify the action for the alarm to take when it reaches the rising threshold:

- *none* — no action takes place
- *event* — an SNMP trap is generated
- *disable port*— the port is disabled
- *disable port/notify* — the port is disabled and an SNMP trap is generated
- *blip* — the broadcast and multicast traffic on the port is blocked for 5 seconds
- *blip port/notify* — the broadcast and multicast traffic on the port is blocked for 5 seconds, and an SNMP trap is generated

If user defined *appears as an option in the Rising Action field, an unrecognized action has been specified using a MIB browser. You cannot select this option.*

Falling Action *none / event / enable / event + enable* Use this field to specify the action for the alarm to take when it reaches the falling threshold:

- *none* — no action takes place
- *event* — an SNMP trap is generated
- *enable* — the port is enabled
- *event + enable* — the port is enabled and an SNMP trap is generated

If user defined *appears as an option in the Falling Action field, an unrecognized action has been specified using a MIB browser. You cannot select this option.*

You should be aware of the following points when using Broadcast Storm Control:

- *The Switch takes 5–7 seconds to recognize that a broadcast storm is occurring.*
- *Broadcast Storm Control calculates the average broadcast bandwidth over the previous 20-second interval. The average is based on four samples taken at 5-second intervals.*
- *When the average value exceeds the rising threshold value, the rising action is triggered. The action is not triggered again until the average broadcast bandwidth falls below the falling threshold level.*

Setting Up the Switch Database (SDB)

The Switch maintains a database of device addresses that it receives on its ports. It uses the information in this database to decide whether a frame should be forwarded or filtered. The database holds up to a maximum of 4080 entries; each entry consists of the MAC address of the device and an identifier for the port on which it was received.

If you have set up Traps for the Switch, notification that the database is becoming full is provided by two traps:

- Database is 90% full
- Database is 100% full

These traps indicate that the maximum number of devices which can be connected to the Switch has been reached. You cannot connect any more devices to the Switch.

Entries are added into the Switch Database in two ways:

- The Switch can learn entries. That is, the unit updates the SDB with the source MAC address, and the port identifier on which the source MAC address is seen.
- The system administrator can enter and update entries using a MIB browser, an SNMP Network Manager or the Switch Database screen described in the following sections.

There are three types of entries in the SDB:

- **Ageing entries** — Initially, all entries in the database are ageing entries. Entries in the database are removed (aged out) if, after a period of time (ageing time), the device has not transmitted. This prevents the database from becoming full with obsolete entries by ensuring that when a device is removed from the network, its entry is deleted from the database. Ageing entries are deleted from the database if the Switch is reset or a power-off/on cycle occurs. For more information about setting an ageing time, refer to "Setting Up the Switch Unit" on page 4-9.
- **Non-ageing entries** — If the ageing time is set to 0:00, all ageing entries in the database are defined as non-ageing entries. This means that they do not age, but they are still deleted if the Switch is reset or a power-off/on cycle occurs. For more information about setting an ageing time, refer to "Setting Up the Switch Unit" on page 4-9.
- **Permanent entries** — Permanent entries do not age, and they are retained in the database if the Switch is reset or a power-off/on cycle occurs.

The Database View

The Unit Database View screen, as shown in Figure 4-12, allows you to view and configure the Switch Database. To access this screen, display the Switch Management screen, choose the management level *Unit*, then select the SDB button.

The Unit Database View screen shows the following:

Database Entries This read-only field shows the number of entries currently in the SDB. The database holds a maximum of 4080 addresses.

MAC Address If you highlight an entry in the listbox and press [Return], this field shows the MAC address for the entry.

Port Number If you highlight an entry in the listbox, this field shows the port identifier for the entry.

Permanent *Yes / No* This field allows you to specify that the current entry is permanent. Refer to the previous section "Setting Up the Switch Database (SDB)" for a description of permanent and ageing entries.

You cannot specify that the current entry is permanent if the port uses AutoSelect VLAN Mode. For more information, refer to "Using AutoSelect VLAN Mode" on page 5-4.

A listbox containing the following three fields:

Port The port ID for the entry.

MAC Address The MAC address for the port currently stored in the database.

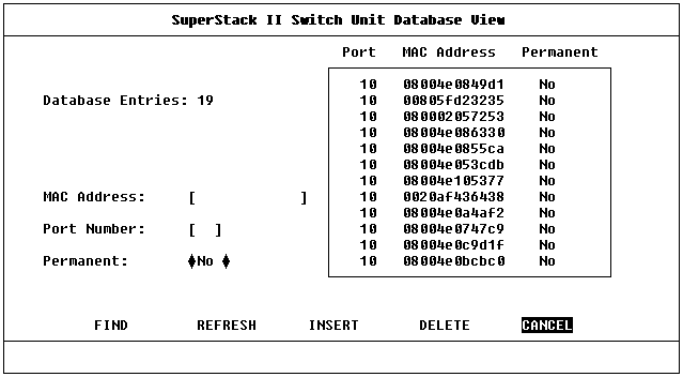


Figure 4-12 Unit Database View screen

Permanent *Yes / No* Shows Yes if this entry is permanent, or No if this entry is ageing or non-ageing.

FIND This button lets you locate an entry in the database. Refer to "Searching the Switch Database" on page 4-17.

REFRESH This button refreshes the database so that it displays the latest information.

INSERT This button lets you insert an entry into the database.

You cannot insert an entry for a port which uses AutoSelect VLAN Mode.

DELETE This button allows you to delete entries from the database.

You cannot delete an entry if it is associated with a port which uses AutoSelect VLAN Mode.

Searching the Switch Database

You can search the switch database in two ways: by MAC address or port number.

By MAC Address

To locate the port number against which a particular MAC address is entered in the SDB:

1. In the MAC Address field, type in the MAC address you are trying to locate.
2. Select FIND. The port ID is displayed in the Port Number field and the entry in the listbox is highlighted with an asterisk (*).

By Port

To locate the MAC addresses entered against a particular port in the SDB:

1. Clear the MAC Address field by moving into the field and pressing the spacebar.
2. In the Port Number field, enter the port ID for which you want MAC addresses displayed.
3. Select FIND. The listbox will show entries in the database for that port only.

Adding an Entry into the SDB

1. In the MAC Address field, type in the MAC address of the device.
2. In the Port Number field, type in the port identifier for this device.
3. Select whether the entry is permanent or not by specifying Yes or No in the Permanent field.
4. Select INSERT.

Deleting an Entry from the SDB

1. In the listbox, highlight the entry you want to delete and press [Return], or type the MAC address into the MAC Address field.
2. Select DELETE.

Specifying that an Entry is Permanent

1. In the listbox, highlight the entry you want to make permanent and press [Return], or type the MAC address into the MAC Address field.
2. In the Permanent field, specify Yes.
3. Select INSERT.

Setting Up Resilient Links

You can configure a Switch to provide resilient links to another device so that network disruption is minimized if a link fails. A *resilient link pair* consists of a main link and a standby link. You define a resilient link pair by specifying the main port and standby port at one end of the pair.

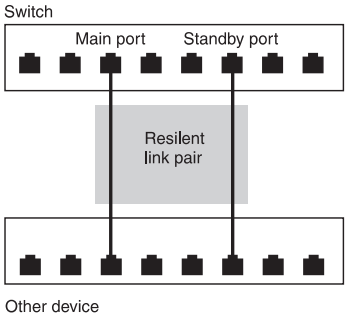


Figure 4-13 Resilient link pair

Under normal network operating conditions, the main link carries your data. The Receive Idle signal of a fiber link or the Test Pulse on an Ethernet twisted pair link is continually monitored by the Switch. If a signal loss is detected, the Switch immediately enables the standby port so that it carries the data. In addition, the main port is disabled.

If a main link has a higher bandwidth than its standby link, traffic is automatically switched back to the main link provided no loss of link is detected for two minutes. Otherwise, you need to manually switch traffic back to the main link.

When setting up resilient links, you should note the following:

- Up to four resilient link pairs can be configured on a Switch 3000 FX.
- Resilient links cannot be set up if Spanning Tree (STP) is enabled on the Switch.
- Resilient links can only be set up on fiber or twisted pair links. The main and standby links in the same pair, however, can use any combination of these media.
- A resilient link pair can only be set up if:
  - The ports belong to the same VLAN.
  - Neither of the ports forms part of another resilient link pair.
- If the main port is a Virtual Lan Trunk (VLT) port, the standby port must also be a VLT port.
- A resilient link pair must be defined at only one end of the connection.
- You cannot disable any port that is part of a resilient link pair.

Configuring Resilient Links

With the Switch Management screen displayed, choose the port to be the main port in the resilient link pair, then select the RESILIENCE button.

The Port Resilience screen is displayed as shown in Figure 4-14. This screen allows you to setup, edit and delete resilient link pairs.

The screen shows the following:

Main Port ID This read-only field displays the ID of the main port.

Media Type *Twisted Pair / Fiber* This read-only field displays the media type connected to the main port.

Link State *Available / Not Available / Not Present* This read-only field displays the connection state of the main port:

- *Available* — The port is operating normally
- *Not Available* — The resilient link pair is disabled
- *Not Present* — The port is not present in the current hardware

Standby Port ID This field shows the current standby port ID and allows you to enter a new port ID. The standby port must be in the same VLAN as the main port.

Media Type *Twisted Pair / Fiber* This read-only field displays the standby port media type.

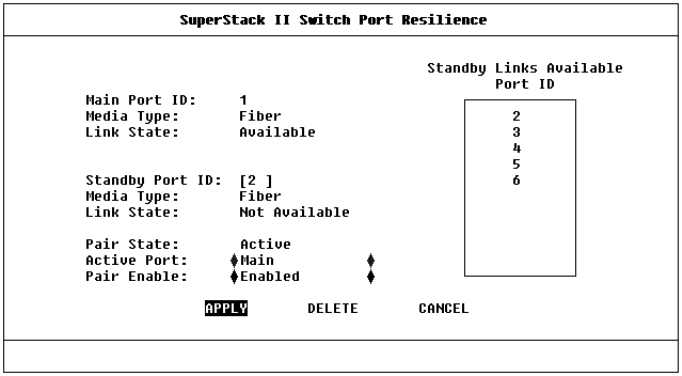


Figure 4-14 Port Resilience screen

Link State *Available / Not Available / Not Present* This read-only field displays the connection state of the standby port:

- *Available* — The port is operating normally
- *Not Available* — The resilient link pair is disabled
- *Not Present* — The port is not present in the current hardware

Standby Links Available This listbox shows the ports that you can configure as standby.

Pair State *Active / Both Failed / Unknown / Not Available* This read-only field displays the current operating state of the resilient link pair:

- *Active* — The resilient link pair is enabled and operating normally with both main and standby port capable of carrying traffic.

- *Both Failed* — Although the resilient link is correctly configured, both links have failed. This could be due to loose connections or cable damage.
- *Unknown* — The network configuration has changed and the resilient link pair no longer conforms to the rules.
- *Not Available* — The resilient link pair is disabled.

Active Port *Main* / *Standby* If a main link does *not* have a higher bandwidth than its standby link, traffic is *not* automatically switched back to the main link when it recovers. Use this field to manually switch traffic back to the main link.

Pair Enable *Enabled* / *Disabled* Use this field to enable or disable the resilient link pair. Before you disable a resilient link pair, you must remove cabling from the ports to avoid creating loops in your network configuration.

Creating a Resilient Link Pair

1. Ensure that the port nominated as the standby port is not physically connected to the unit.
2. Ensure both ports have an identical port security mode configuration and that they are members of the same VLAN.
3. At the Switch Management screen, select the port to be configured as the main port in the link. Select the RESILIENCE button at the foot of the screen.
4. Select the standby port from the Standby Links Available listbox or enter the port ID in the Standby Port ID field.
5. Enable the pair in the Pair Enabled field. Select APPLY.
6. Connect the cabling for the standby port.

Deleting a Resilient Link Pair

To delete the resilient link set up on the port, select the DELETE button at the foot of the screen. The Port Resilience screen closes and the Switch Management screen is displayed.

Viewing the Resilient Setup

With the Switch Management screen displayed, choose the management level *Unit* and select the RESILIENCE button.

The Unit Resilience Summary screen is displayed as shown in Figure 4-15. This screen shows the current resilient link configuration for the unit, and allows you to access the Port Resilience screen for resilient link pairs.

The following read-only information is displayed:

MAIN Port This read-only field displays the ID of the port configured as the main port for the resilient link pair.

STANDBY Port This read-only field displays the ID of the port configured as the standby port for the resilient link pair.

Pair State *Active / Both Failed / Unknown / Not Available* This read-only field displays the current state of the resilient link pair:

- *Active* — The resilient link pair is enabled and operating normally with both main and standby ports capable of carrying traffic.
- *Both Failed* — Although the resilient link is correctly configured, both links have failed. Check for any loose connections or cable damage.
- *Unknown* — The network configuration has changed and the resilient link pair no longer conforms to the rules.
- *Not Available* — The resilient link pair is disabled.

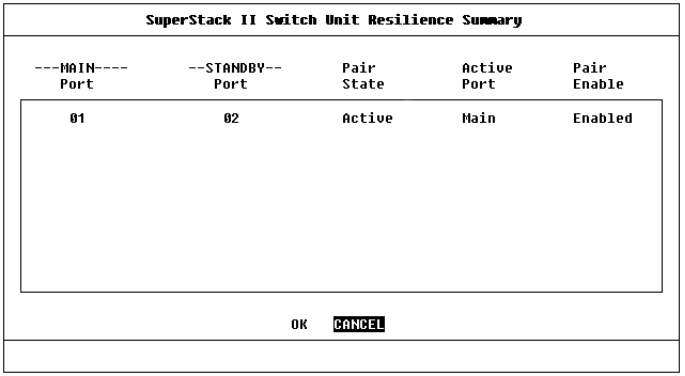


Figure 4-15 Unit Resilience Summary screen

Active Port *Main / Standby / Both Failed* This read-only field displays which port in the resilient link pair is currently carrying traffic:

- *Main* — The pair is operating in its normal state with the main port carrying traffic.
- *Standby* — The main port has failed and the standby port is carrying the traffic. You should rectify the fault as soon as possible. If a main port has a higher bandwidth than the standby port, traffic is automatically switched back provided no loss of link is detected for two minutes. Otherwise, switch the traffic back manually by setting the Active Port field in the Port Resilience screen (described on page 4-19) to Main.
- *Both Failed* — Both ports of the resilient link pair have failed. This could be due to loose connections or cable damage.

Pair Enable *Enabled* / *Disabled* This read-only field displays whether the resilient link pair is currently enabled or disabled. You enable or disable a resilient link pair using the Port Resilience screen described in "Configuring Resilient Links" on page 4-19.

OK This button allows you to access the Port Resilience screen for the current resilient link pair.

Setting Up Traps

Traps are messages sent across the network to an SNMP Network Manager. They alert the network administrator to faults or changes at the Switch device.

Your Network Manager may automatically set up traps in the Switch Trap Table. Check the documentation accompanying the network management software.

To access the Trap Setup screen, select the SETUP TRAPS button from the Management Setup screen (described in Chapter 3). The Trap Setup screen is shown in Figure 4-16.

The screen shows the following:

IP or IPX Address This field allows you to enter the IP or IPX address of the remote network management stations to which traps should be sent.

Community String This field allows you to enter community strings for each remote Network Manager, allowing a very simple method of authentication between the Switch and the remote Network Manager. The text string can be of 32 characters or less. If you want a Network Manager to receive traps generated by the device, you must enter the community string of the Network Manager into the trap table. The default community string is *public*.

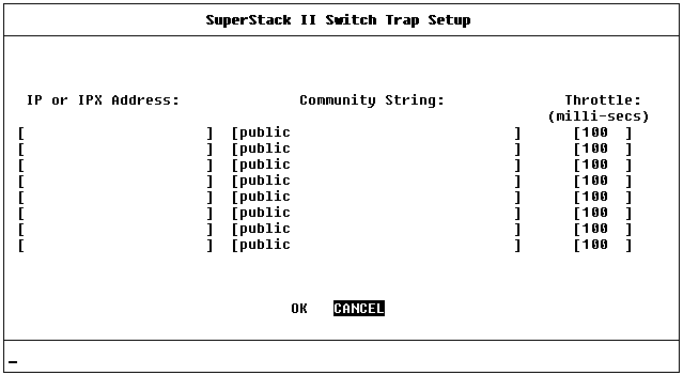

SuperStack II Switch Trap Setup
IP or IPX Address:
Community String:
Throttle:
(milli-secs)
[ ] [public] [100]
[ ] [public] [100]
[ ] [public] [100]
[ ] [public] [100]
[ ] [public] [100]
[ ] [public] [100]
[ ] [public] [100]
[ ] [public] [100]
OK
CANCEL

Figure 4-16 Trap Setup screen

Throttle This field allows you to specify a throttle delay value for each remote Network Manager. Throttle delays are time periods placed between packets to prevent a remote Network Manager receiving too many traps at once. The unit of throttle is one thousandth of a second. The default value is 100, which gives a delay of one tenth of a second between each packet transmission.

Setting Up the Console Port

From the Management Setup screen, described in Chapter 3, select the CONSOLE PORT button. The Console Port Setup screen is displayed, as shown in Figure 4-17.

If you change any of the console port parameters, you terminate any existing sessions using the console port when you exit the screen. Ensure that the connected equipment's console port parameters are set to match the new configuration. This allows you to continue to access the management facility from the equipment after you change the console port parameters.

The screen shows the following:

Connection Type *Local / Remote* This field allows you to select the type of console port connection. Select *Remote* if you want to manage the Switch via a modem; DCD Control and DSR Control are enabled. For all other cases, this field should be set to *Local*.

DCD Control *Enabled / Disabled* This field is only applicable to local connection types. It determines if DCD is required for a local connection, and whether the connection is closed if DCD is removed. Refer to your terminal or modem user documentation if you are unsure of the correct setting.

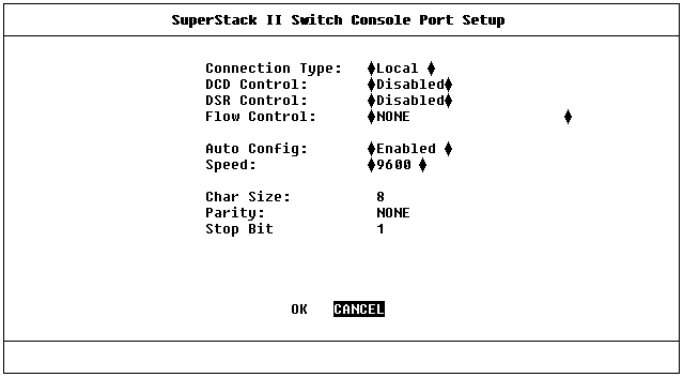


Figure 4-17 Console Port Setup screen

DSR Control *Enabled / Disabled* This field is only applicable to local connection types. It determines if DSR is required for a local connection, and whether the connection is closed if DSR is removed. Refer to your terminal or modem user documentation if you are unsure of the correct setting.

Flow Control *XON/XOFF / NONE / RTS-CTS Unidirectional / RTS-CTS Bidirectional* This field allows you to select the correct flow control option for your terminal or modem. Refer to your terminal or modem user documentation if you are unsure of the correct setting.

Auto Config *Enabled / Disabled* The Switch can auto-configure the line speed (baud rate) of the console port to work with your VT100 terminal. This field allows you to specify whether auto-configuration is enabled.

Speed *1200 / 2400 / 4800 / 9600 / 19200* This field allows you to select the correct line speed (baud rate) for your terminal or modem. If you have enabled auto-configuration, the line speed is set automatically.

Char Size *8* This read-only field displays the character bit (data bit) size for the Switch. You should set your terminal to the same value.

Parity *NONE* This read-only field displays the parity setting for the Switch. You should configure your terminal to the same setting.

Stop Bit *1* This read-only field displays the stop bit setting for the Switch. You should configure your terminal to the same setting.

Resetting the Switch 3000 FX

If you suspect a problem with the Switch, you can reset it.

1 From the Main Menu, select the RESET option.

The Reset screen is displayed as shown in Figure 4-18.

2 Select OK.

Resetting the Switch in this way is similar to performing a power-off/on cycle. No setup information is lost.

CAUTION: *Performing a reset may cause some of the data being transmitted at that moment to be lost.*

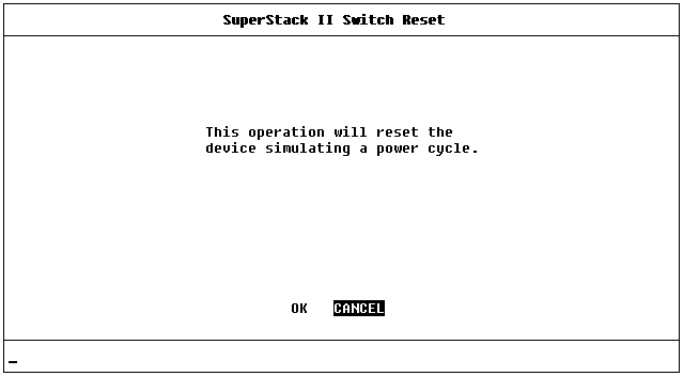


Figure 4-18 Reset screen

Initializing the Switch 3000 FX

This screen allows you to perform a reset as described in the previous section, and in addition, returns non-volatile data stored on the unit to its factory defaults (shown on page 1-12). Note that the IP address is not cleared. You should only initialize the Switch if:

- The configuration of the device no longer suits your network.
- Other efforts to solve problems have not succeeded.

To initialize the Switch:

1 From the Main Menu, select the INITIALIZE option.

The Initialize screen is displayed as shown in Figure 4-19.

2 Select OK.

CAUTION: *Use the Initialize option with great care. The Switch configuration is cleared from memory and cannot be recovered. After initialization, all user information is lost and only default users are available. All ports are set to their default values, and are therefore enabled and available to all users.*

When initializing the Switch, take particular note of the following:

- Network loops occur if you have set up resilient links. Before initializing the Switch, ensure you have disconnected the cabling for all your standby links.

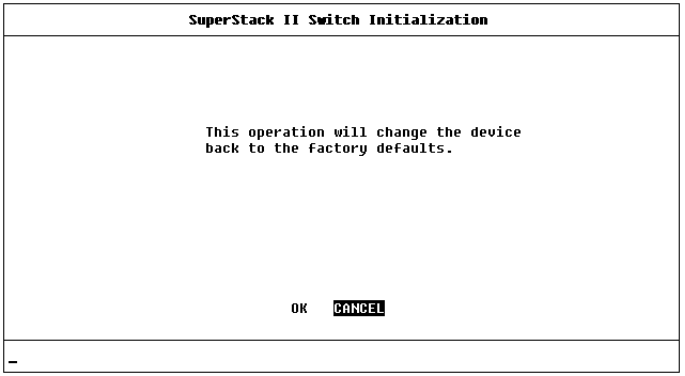


Figure 4-19 Initialize screen

- VLT ports fail and you are not able to manage the Switch if your management station communicates via the VLT. To avoid this:

a Remove the VLT configuration from both ends of the VLT link before you initialize the Switch. Note that the port furthest from your management station should have its VLT configuration removed first.

b Reconfigure the VLT once the initialization is complete.

Upgrading Software

When 3Com issues a new version of the software image for the Switch, you can obtain it from 3Com's information delivery systems, described in "Online Technical Services" on page F-1.

For upgrading the ATM OC-3c Module software, refer to the "SuperStack II Switch ATM OC-3c Module User Guide".

You use the Software Upgrade screen to download new software images. The protocol used for downloading software images is TFTP running over UDP/IP or IPX.

CAUTION: *Before attempting to download, note:*

- *The download only works over the network; it does not work through the console port.*
- *The download does not work over a Virtual LAN Trunk (VLT) if you have a Boot software version lower than version 2.0.*
- *The download does not work over an ATM link.*

To upgrade Switch management software:

1 From the Main Menu, select SOFTWARE UPGRADE.

The Software Upgrade screen is displayed, as shown in Figure 4-20.

2 From the Destination field, select Switch (this is the default).

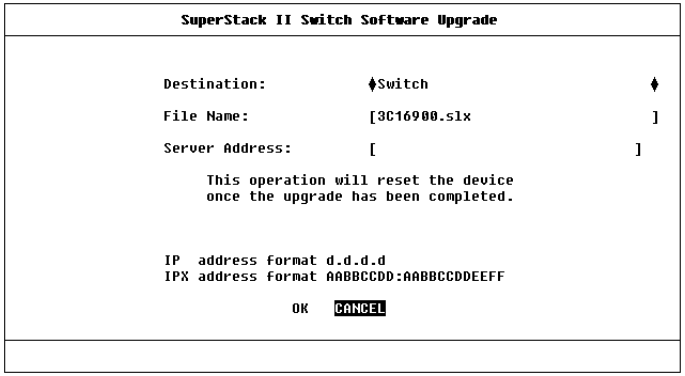

SuperStack II Switch Software Upgrade
Destination: ♦Switch ♦
File Name: [3C16900.slx]
Server Address: [ ]
This operation will reset the device
once the upgrade has been completed.
IP address format d.d.d.d
IPX address format AABBCCDD:AABBCCDDEEFF
OK CANCEL

Figure 4-20 Software Upgrade screen

3 In the File Name field, enter the name of the file that contains the software image to be downloaded to the Switch.

You must place the image file where it is accessible to the TFTP load request. Check with your system administrator if you are unsure of where to place the image file.

4 In the Server Address field, enter the IP or IPX address of the server containing the software image to be loaded.

5 Select OK.

During the download, the MGMT LED flashes green and the screen is locked. When the download is complete, the Switch is reset.

5 ADVANCED MANAGEMENT

Virtual LANs (VLANs)

Setting up Virtual Local Area Networks (VLANs) on the Switch 3000 FX provides you with less time-consuming network administration and more efficient network operation.

The following sections explain more about the concept of VLANs and explain how they can be implemented on the Switch 3000 FX.

What are VLANs?

A VLAN is defined as a group of location- and topology-independent devices that communicate as if they are on the same physical LAN. This means that LAN segments are not restricted by the hardware which physically connects them; the segments are defined by flexible user groups that you create using software.

With VLANs, you can define your network according to:

- **Departmental groups** — For example, you can have one VLAN for the Marketing department, another for the Finance department, and another for the Development department.
- **Hierarchical groups** — For example, you can have one VLAN for directors, another for managers, and another for general staff.
- **Usage Groups** — For example, you can have one VLAN for users of e-mail, and another for users of multimedia.

Benefits of VLANs

Implementing VLANs on your network has three main advantages:

- It eases the change and movement of devices on IP networks
- It helps to control broadcast traffic
- It provides extra security

How VLANs Ease Change and Movement

With traditional IP networks, network administrators spend much of their time dealing with moves and changes. If users move to a different IP subnet, the IP addresses of each endstation must be updated manually.

With a VLAN setup, if an endstation in VLAN 1 is moved to a port in another part of the network, you only need to specify that the new port is in VLAN 1. This is something that can be done automatically if you have 3Com's Transcend® Enterprise Manager for Windows (v6.0 and above).

How VLANs Control Broadcast Traffic

With traditional networks, congestion can be caused by broadcast traffic which is directed to all network devices whether they require it or not. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices which need to communicate with each other.

How VLANs Provide Extra Security

Devices within each VLAN can only communicate with devices in the same VLAN. If a device in VLAN 1 needs to communicate with devices in VLAN 2, the traffic must cross a router.

An Example

Figure 5-1 shows a network configured with three VLANs — one for each of the departments that access the network. The membership of VLAN 1 is restricted to ports 1, 2, 3, 4 and 5 of Switch A; membership of VLAN 2 is restricted to ports 4, 5, 6, 7 and 8 of Switch B while VLAN 3 spans both Switches containing ports 6, 7 and 8 of Switch A, and 1, 2 and 3 of Switch B.

In this simple example, each of these VLANs can be seen as a *broadcast domain* — physical LAN segments that are not constrained by their physical location.

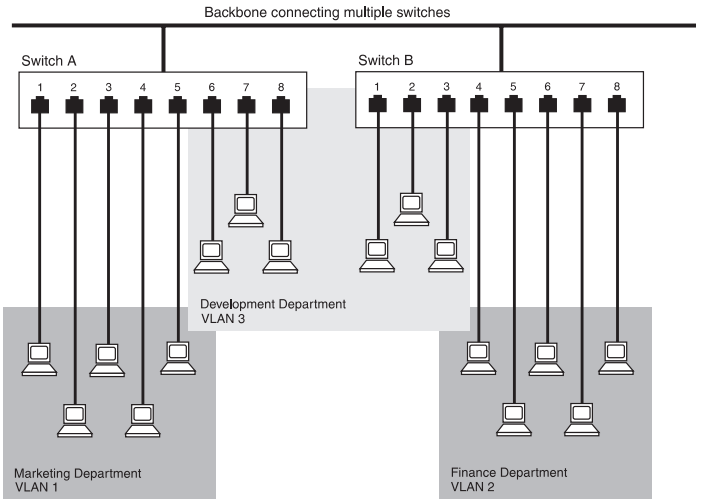


Figure 5-1 The concept of VLANs

VLANs and the Switch 3000 FX

The Switch 3000 FX supports VLANs which consist of a set of switch ports. Each switch port can only belong to one VLAN at a time, regardless of the device to which it is attached.

Each Switch 3000 FX can support up to 16 VLANs. However, you can have more than 16 VLANs in your entire network; to do this, you connect the 16 Switch VLANs to other VLANs using a router.

The Default VLAN and Moving Ports From the Default VLAN

On each Switch, VLAN 1 is the Default VLAN of the Switch; it has two properties:

- It contains all the ports on a new or initialized Switch
- It is the only VLAN which allows an SNMP Network Manager to access the management agent of the unit

By default, if a device is attached to a port in the Default VLAN and you want to move the device into another VLAN, you need to use the VLAN Setup screen to place the port in that VLAN. For more information about the VLAN Setup screen, refer to "Setting Up VLANs on the Switch" on page 5-8.

Connecting VLANs to a Router

If the devices in a VLAN need to talk to devices in a different VLAN, each VLAN requires a connection to a router. Communication between VLANs can only take place if they are all connected to the router. A VLAN not connected to a router is an isolated VLAN. You need one port for each VLAN connected to the router.

Connecting Common VLANs Between Switch Units

If you want to connect the VLANs on the Switch 3000 FX with the same VLANs on another Switch unit, you can set up one link per VLAN. Alternatively, you can set up a single link for all the VLANs by creating a *Virtual LAN Trunk* (VLT). A VLT is a Switch-to-Switch link which carries traffic for all the VLANs on each Switch. To set up a VLT, you configure the port at each end of the link.

VLTs can only be used for links between SuperStack® II Switch 1000, Switch 3000 and Desktop Switch units. You cannot use VLTs for Switch–router links.

If you specify that a port on one VLAN is a VLT port, that port carries traffic for all the VLANs on the Switch. If you then disable the VLT function on that port, the port only carries traffic for the Default VLAN (VLAN 1).

Using AutoSelect VLAN Mode

By default, all ports on the Switch use Port VLAN Mode — where each switch port is *manually* placed in the required VLAN. The Switch allows some ports to use another mode, AutoSelect VLAN Mode. In this mode, the ports are *automatically* placed in the required VLAN by referring to a VLAN Server database in 3Com's Transcend Enterprise Manager v6.0 for Windows.

AutoSelect VLAN Mode works as follows:

1 When an endstation is connected to a Switch or moves from one port to another, the Switch learns the MAC address of the endstation.

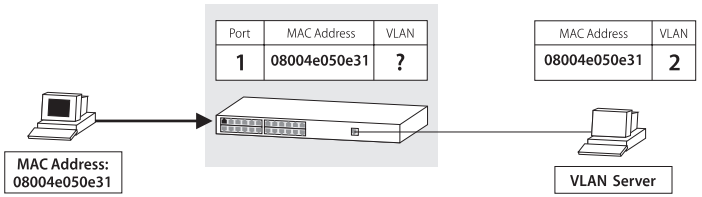


Figure 5-2 Switch learns the endstation's MAC address

2 If the relevant port uses AutoSelect VLAN Mode, the Switch refers to the VLAN Server to determine the VLAN membership of the endstation.

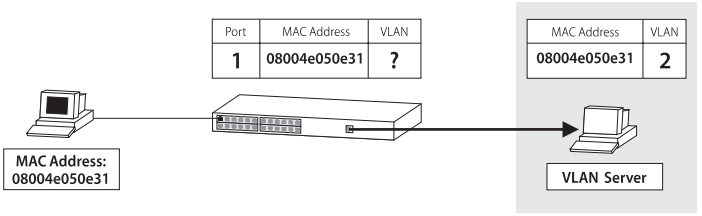


Figure 5-3 Switch refers to the VLAN Server

3 Having obtained the VLAN membership for the endstation, the Switch places the relevant port in the specified VLAN.

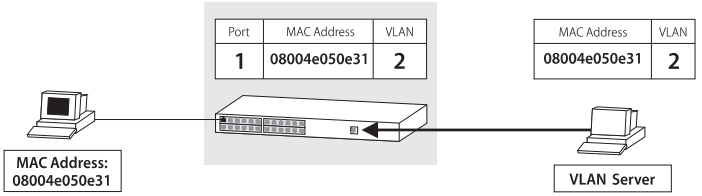


Figure 5-4 Switch places the port in the VLAN

AutoSelect VLAN Mode has an advantage over Port VLAN Mode because once the VLAN Server database is set up correctly, you can move endstations to other ports or other Switch units and the VLAN allocation of each endstation is automatically configured.

If you use AutoSelect VLAN Mode, note the following:

- You need to specify an IP address and community string for the VLAN Server.
- You cannot use VLAN 15.
- If a port has been configured as a backbone port or as a VLT port, the port cannot use AutoSelect VLAN Mode.
- If a port has a permanent address stored against it in the Switch Database, the port cannot use AutoSelect VLAN Mode.
- We recommend that you connect each switch port to a single endstation. If you want to connect a port to multiple endstations, specify that the port uses Port VLAN Mode.

For information about how to set up VLANs using AutoSelect VLAN Mode, refer to "Setting Up VLANs Using AutoSelect VLAN Mode" on page 5-10.

For more information about the VLAN Server database, refer to the documentation supplied with 3Com's Transcend Enterprise Manager.

Using Non-routable Protocols

If you are running non-routable protocols on your network (for example, DEC LAT or NET BIOS), devices within one VLAN are not able to communicate with devices in a different VLAN.

Using Unique MAC Addresses

If you connect a server with multiple network adapters to the Switch, we recommend that you configure each network adapter with a unique MAC address.

Extending VLANs into an ATM Network

If the Switch has an ATM OC-3c Module installed, you can extend the VLANs you have defined in your existing network into an ATM network. For more information, refer to the "*SuperStack II Switch ATM OC-3c Module User Guide*".

VLAN Configuration Example

The example shown in Figure 5-5 illustrates two VLANs spanning three Switch 1000 units and a basement Switch 3000 FX unit with a Plug-in Module. Each Switch 1000 connects to the basement Switch using a VLT. The attached router allows the two VLANs to communicate with each other.

To set up this configuration:

1. Use the VT100 screens or VLAN Server database to:
   - **a** Place ports 1–6 and 13–18 of all the Switch 1000 units in VLAN 1.
   - **b** Place ports 7–12 and 19–24 of all the Switch 1000 units in VLAN 2.
2. Connect a port on each Switch 1000 to a port in the Switch 3000 FX.
3. Use the VT100 screens to:
   - **a** Specify that each Switch 1000 port connected to the Switch 3000 FX is a backbone port. For more information about backbone ports, refer to the *"SuperStack II Switch 1000 User Guide"*.
   - **b** Specify that each Switch 1000 port connected to the Switch 3000 FX is a VLT port.
   - **c** Specify that each Switch 3000 FX port connected to a Switch 1000 is a VLT port.
4. Connect port 1 of the Switch 3000 FX to Server 1.
5. Connect port 2 of the Switch 3000 FX to Server 2.
6. Use the VT100 screens or VLAN Server database to:
   - **a** Place port 1 of the Switch 3000 FX in VLAN 1.
   - **b** Place port 2 of the Switch 3000 FX in VLAN 2.
7. Connect two spare ports on the Switch 3000 FX to the router.
8. Use the VT100 screens or VLAN Server database to specify that one Switch 3000 FX port connected to the router is placed in VLAN 1, and the other is placed in VLAN 2.

You can set up this configuration more easily if you use 3Com's Transcend Enterprise Manager applications for all the management tasks.

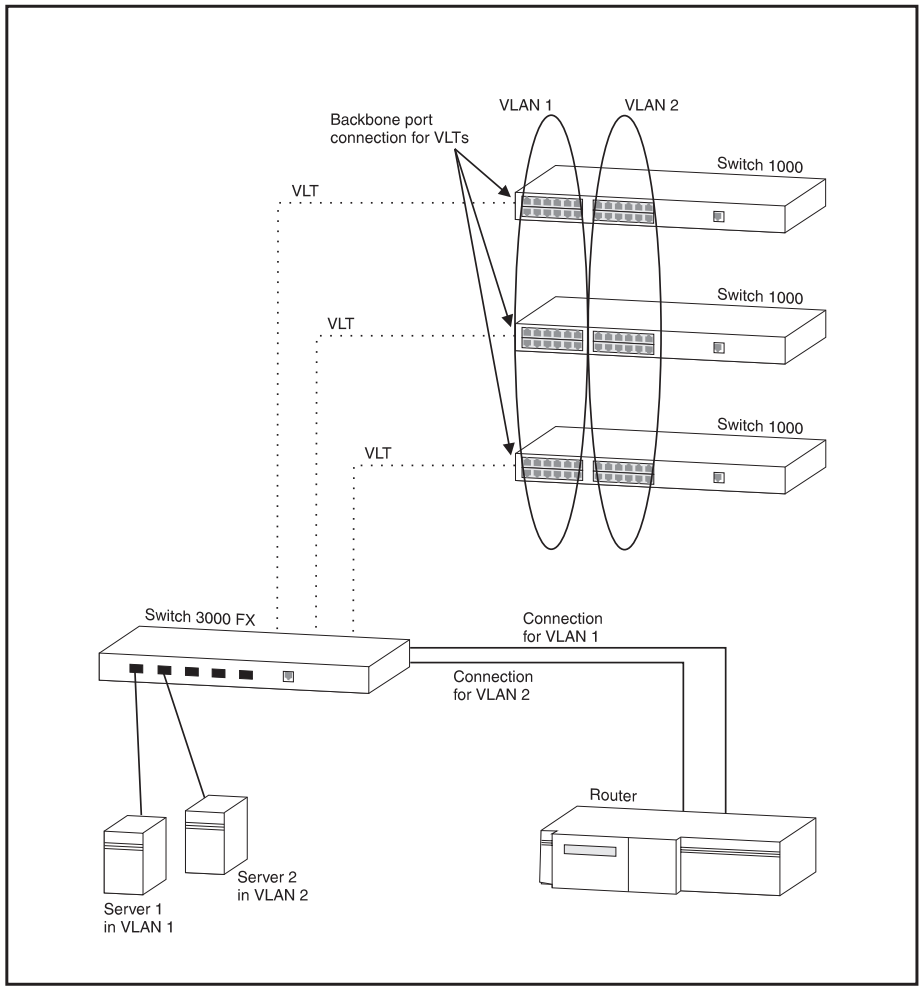


Figure 5-5 VLAN configuration with a Switch 3000 FX as a basement switch

Setting Up VLANs on the Switch

The VLAN Setup screen allows you to:

- Assign ports to VLANs, if those ports use Port VLAN Mode.
- View VLAN setup information for the Switch.

To access the VLAN Setup screen:

1. From the Main Menu, select SWITCH MANAGEMENT. The Switch Management screen is displayed.
2. In the Management Level field, choose *VLAN*.
3. Choose the SETUP button. The VLAN Setup screen is displayed, as shown in Figure 5-6.

The screen shows the following:

A listbox containing three fields:

Port This field allows you to select the ID of the port that you want to set up.

Type *VLT / Standby / ATM / AutoSelect* This field displays information about the setup of the port:

- *VLT* — The port is a VLT port. A Virtual LAN Trunk (or VLT) is a Switch-to-Switch link which carries traffic for all the VLANs on each Switch. For more information about VLTs in general, refer to "VLANs and the Switch 3000 FX" on page 5-3. To specify that a port is a VLT port, refer to "Setting Up the Switch Ports" on page 4-11.

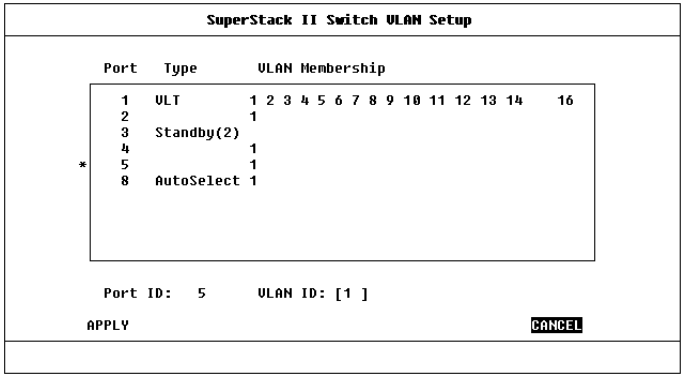

SuperStack II Switch VLAN Setup
Port Type VLAN Membership
1 VLT 1 2 3 4 5 6 7 8 9 10 11 12 13 14 16
2 1
3 Standby(2)
4 1
* 5 1
8 AutoSelect 1
Port ID: 5 VLAN ID: [1]
APPLY
CANCEL

Figure 5-6 VLAN Setup screen

- *Standby* — The port is the standby port of a resilient link pair. The main port of the pair is displayed in brackets. For more information about resilient links, refer to "Setting Up Resilient Links" on page 4-18.
- *ATM* — The port is an ATM OC-3c Module port. For more information, refer to the "*SuperStack II Switch ATM OC-3c Module User Guide*".
- *AutoSelect* — The port uses AutoSelect VLAN Mode. For more information about AutoSelect VLAN Mode, refer to "Using AutoSelect VLAN Mode" on page 5-4. For information about how to configure VLANs using AutoSelect VLAN Mode, refer to "Setting Up VLANs Using AutoSelect VLAN Mode" on page 5-10.

VLAN Membership This field displays the ID of the VLAN(s) to which the port belongs.

Port ID *1 / 2 / 3 ... 6 / 7 / 8* This field displays the ID of the port currently selected in the listbox.

VLAN ID *1 / 2 / 3 ... 14 / 15 / 16* If the port specified in the Port ID field uses Port VLAN Mode, this field allows you to enter the ID of the VLAN to which the port is to be assigned. If the port uses AutoSelect VLAN Mode, you cannot specify the VLAN ID. By default, all ports use Port VLAN Mode and belong to the Default VLAN (VLAN 1). This field is not displayed if the port is a VLT port.

If one or more ports use AutoSelect VLAN Mode, you cannot use VLAN 15. Also, if you are using the Spanning Tree Protocol, you cannot use VLAN 16. In these cases, the relevant VLANs are used internally by the Switch and are therefore not available.

APPLY This button applies any changes to the VLAN database.

ATM LEC Setup If the port is an ATM OC-3c Module port, this button allows you access the VLAN LEC Setup screen for extending your VLANs into an ATM network. For more information, refer to the "*SuperStack II Switch ATM OC-3c Module User Guide*".

Assigning a Port to a VLAN When Using Port VLAN Mode

1. In the Port ID field, enter the ID of the required port.
2. In the VLAN ID field, enter the ID of the required VLAN.
3. Select APPLY.

CAUTION: *Initially, all Switch ports belong to the Default VLAN (VLAN 1). This VLAN is the only one that allows an SNMP Network Manager to access the management agent of the unit. If you remove all ports from VLAN 1, an SNMP Network Manager cannot manage the Switch.*

Specifying that a Port is a VLT Port

To specify that a port is a VLT port, refer to "Setting Up the Switch Ports" on page 4-11.

To create a VLT link, the ports on both ends of the link must be VLT ports.

Setting Up VLANs Using AutoSelect VLAN Mode

To set up VLANs using AutoSelect VLAN Mode, you need to:

- Specify information about the VLAN Server
- Specify that the Switch unit, or individual ports on the unit, use AutoSelect VLAN Mode

Specifying Information About the VLAN Server

The VLAN Server screen allows you to specify information about the VLAN Server. To access the VLAN Server screen:

1. From the Main Menu, select SWITCH MANAGEMENT. The Switch Management screen is displayed.
2. In the Management Level field, choose VLAN.
3. Choose the SERVER button. The VLAN Server screen is displayed, as shown in Figure 5-7.

The screen shows the following:

VLAN Server IP Address Enter the IP address of your VLAN Server in this field.

Backup VLAN Server IP Address This field allows you to enter the IP address of a backup VLAN Server. A backup VLAN Server can be used to supply VLAN allocations when the Switch cannot access the main VLAN Server.

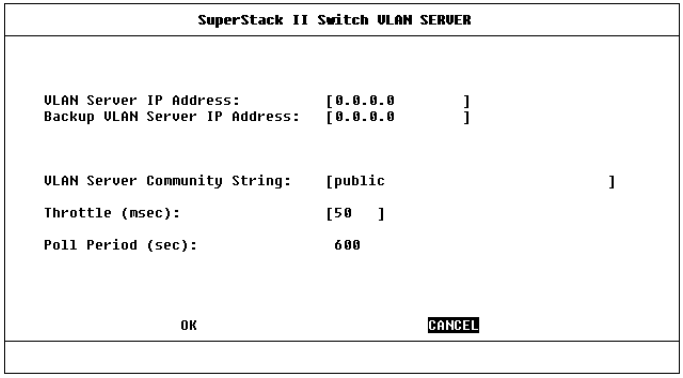

SuperStack II Switch VLAN SERVER
VLAN Server IP Address: [0.0.0.0]
Backup VLAN Server IP Address: [0.0.0.0]
VLAN Server Community String: [public]
Throttle (msec): [50]
Poll Period (sec): 600
OK
CANCEL

Figure 5-7 VLAN Server screen

VLAN Server Community String This field allows you to enter a community string for the VLAN Server(s). The default community string is *public*.

Throttle *0 ... 99999* This field allows you to specify the time delay, in milliseconds, between the transmission of VLAN allocation requests to the Server. The time delay is used to avoid placing an excessive workload on the VLAN Server. The default setting for this field is 50 milliseconds.

Poll Period This read-only field shows the time interval, in seconds, between successive polls of the VLAN Server. The Switch polls the VLAN Server once every poll period to check for any changes.

Specifying AutoSelect VLAN Mode

To specify that the Switch uses AutoSelect VLAN Mode, refer to "Setting Up the Switch Unit" on page 4-9.

To specify that a port on the Switch uses AutoSelect VLAN Mode, refer to "Setting Up the Switch Ports" on page 4-11.

Spanning Tree Protocol

Using the Spanning Tree Protocol (STP) functionality of your Switch makes your network more fault tolerant.

The following sections explain more about STP and the STP features supported by the Switch.

STP is not currently supported over an Asynchronous Transfer Mode (ATM) network. Therefore, if you have an ATM OC-3c Module installed in your Switch, it does not join the STP system.

What is STP?

STP is a part of the 802.1d bridge specification defined by the IEEE Computer Society. To explain STP more effectively, the Switch 3000 FX will be defined as a bridge.

STP is a bridge-based system for providing fault tolerance on networks. STP allows you to implement parallel paths for network traffic, and ensure that:

- Redundant paths are disabled when the main paths are operational
- Redundant paths are enabled if the main paths fail

As an example, Figure 5-8 shows a network containing three LAN segments separated by three bridges. With this configuration, each segment can communicate with the others using two paths. This configuration creates loops which cause the network to overload; however, STP allows you to have this configuration because it detects duplicate paths and immediately prevents, or blocks, one of them from forwarding traffic.

Figure 5-9 shows the result of enabling STP on the bridges in the configuration. The STP system has decided that traffic from LAN segment 2 to LAN segment 1 can only flow through Bridges C and A.

If the link through Bridge C fails, as shown in Figure 5-10, the STP system reconfigures the network so that traffic from segment 2 flows through Bridge B.

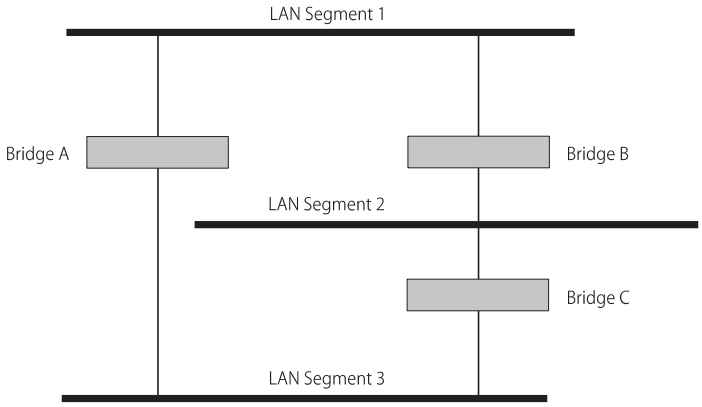


Figure 5-8 A network that creates loops

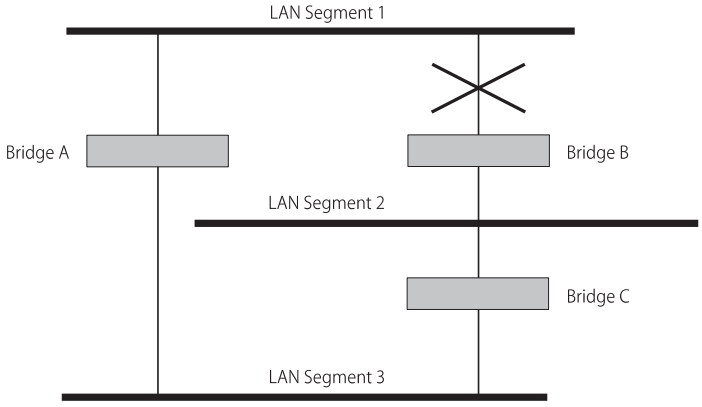


Figure 5-9 Traffic flowing through Bridges C and A

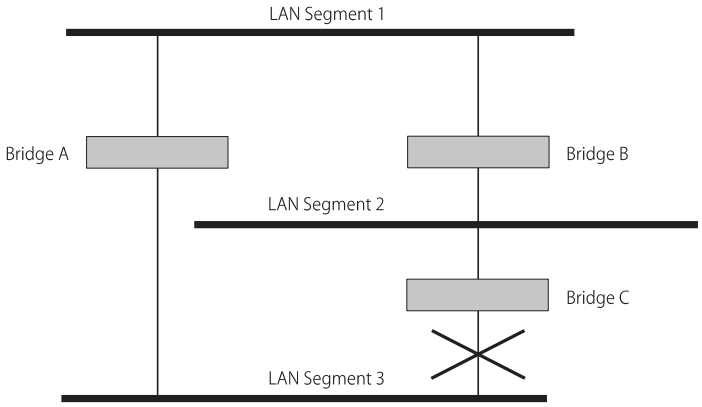


Figure 5-10 Traffic flowing through Bridge B

How STP Works

STP Initialization

Initially, the STP system requires the following before it can configure the network:

- Communication between all the bridges. This communication is carried out using Bridge Protocol Data Units (BPDUs), which are transmitted in packets with a known multicast address.
- One bridge to start as a master or Root Bridge, a central point from which the network is configured.

The Root Bridge is selected on the basis of it having the lowest Bridge Identifier value. This is a combination of the unique MAC address of the bridge and a priority component defined for the bridge.

The Root Bridge generates BPDUs on all ports at a regular interval known as the Hello Time. All other bridges in the network have a Root Port. This is the port nearest to the Root Bridge, and it is used for receiving the BPDUs initiated by the Root Bridge.

STP Stabilization

Once the network has stabilized, two rules apply to the network:

1 Each network segment has one Designated Bridge Port. All traffic destined to pass in the direction of or through the Root Bridge flows through this port. The Designated Bridge Port is the port which has the lowest Root Path Cost for the segment.

The Root Path Cost consists of the path cost of the Root Port of the bridge, plus the path costs across all the Root Ports back to the Root Bridge. Table 5-1 shows the default path costs for the Switch 3000 FX.

Table 5-1 Default path costs

Port Type	Duplex	Cost
100BASE-TX (VLT) / 100BASE-FX (VLT)	Full	5
	Half	12
10BASE-T (VLT)	Half	25
100BASE-TX / 100BASE-FX	Full	150
	Half	300
10BASE-T	Half	650

2 After all the bridges on the network have determined the configuration of their ports, each bridge only forwards traffic between the Root Port and the ports that are the Designated Bridge Ports for each network segment. All other ports are *blocked*, which means that they are prevented from forwarding traffic.

STP Reconfiguration

In the event of a network failure, such as a segment going down, the STP system reconfigures the network to cater for the changes. If the topology of your network changes, the first bridge to detect the change sends out an SNMP trap.

An Example

Figure 5-11 illustrates part of a network. All bridges have a path cost value assigned to each port, identified by PC=xxx (where xxx is the value). Bridge A is selected by STP as the Root Bridge, because it has the lowest Bridge Identifier. The Designated Bridge Port for LAN A is port 1 on Bridge A. Each of the other four bridges have a Root Port (the port closest to the Root Bridge). Bridge X and Bridge B can offer the same path cost to LAN B. In this case Bridge B's port is chosen as the Designated Bridge Port, because it has the lowest Bridge Identifier. Bridge C's port is chosen as the Designated Bridge Port for LAN C because it offers the lowest Root Path Cost (the route through Bridge C and B costs 200, the route through Bridge Y and B would cost 300). You can set the path cost of a bridge port to influence the configuration of a network with a duplicate path.

Once the network topology is stable, all the bridges listen for special Hello BPDUs transmitted from the Root Bridge at regular intervals. If the STP Max Age time of a bridge expires (refer to "Configuring the STP Parameters of VLANs" on page 5-18) before receiving a Hello BPDU, the bridge assumes that the Root Bridge, or a link between itself and the Root Bridge, has gone down. The bridge then initiates a reconfiguration of the network topology.

You can adjust timers to determine how quickly a network reconfigures and therefore how rapidly the network recovers from a path failure (refer to "Configuring the STP Parameters of VLANs" on page 5-18).

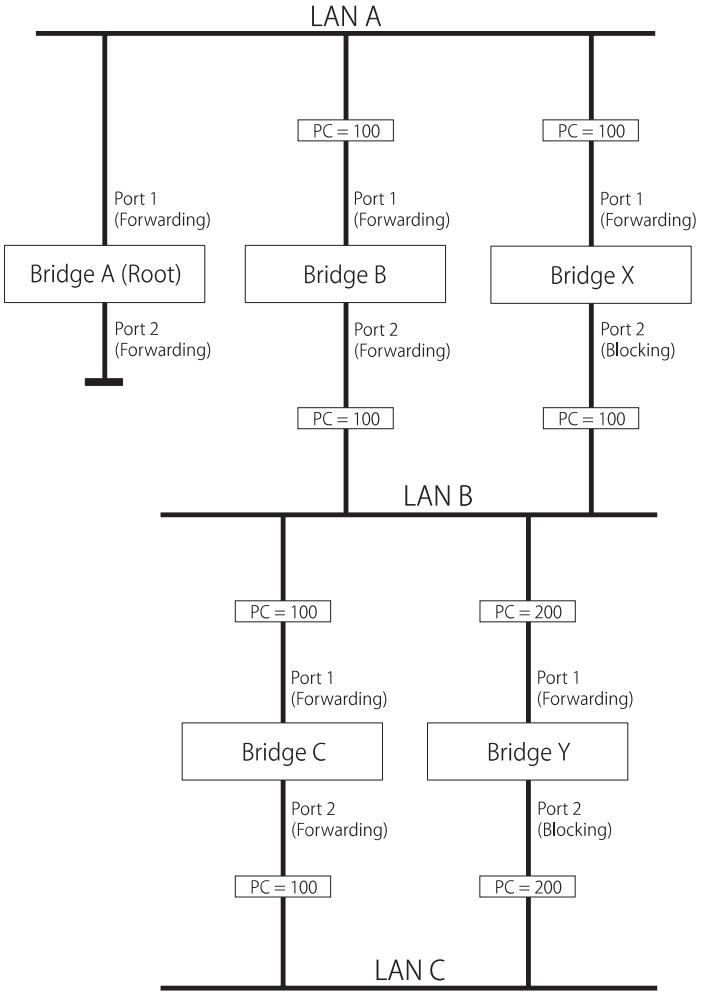


Figure 5-11 Port costs in a network

STP Configurations

Figure 5-12 shows two possible STP configurations using SuperStack II Switch units:

- **Configuration 1 — Redundancy for Backbone Link**

  In this configuration, a Desktop Switch and Switch 3000 FX both have STP enabled and are connected by two Fast Ethernet links. STP discovers a duplicate path and disables one of the links. If the enabled link breaks, the disabled link becomes re-enabled, therefore maintaining connectivity.

- **Configuration 2 — Redundancy through Meshed Backbone**

  In this configuration, four Switch 3000 FX units are connected such that there are multiple paths between them. STP discovers the duplicate paths and disables two of the links. If an enabled link breaks, one of the disabled links becomes re-enabled, therefore maintaining connectivity.

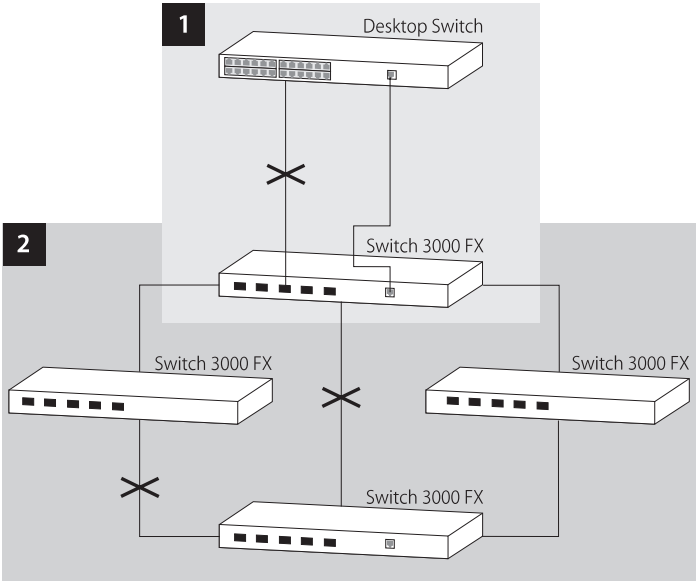


Figure 5-12 STP configurations

Enabling STP on the Switch

To enable STP on your Switch:

1. From the VT100 Main Menu, select SWITCH MANAGEMENT. The Switch Management screen is displayed.
2. In the Management Level field, choose Unit.
3. Choose the SETUP button. The Unit Setup screen is displayed as shown in Figure 5-13.
4. In the Spanning Tree field, specify Enable.
5. Choose OK.

You cannot enable STP if you have set up resilient links on any of the Switch ports, or if you are using VLAN 16.

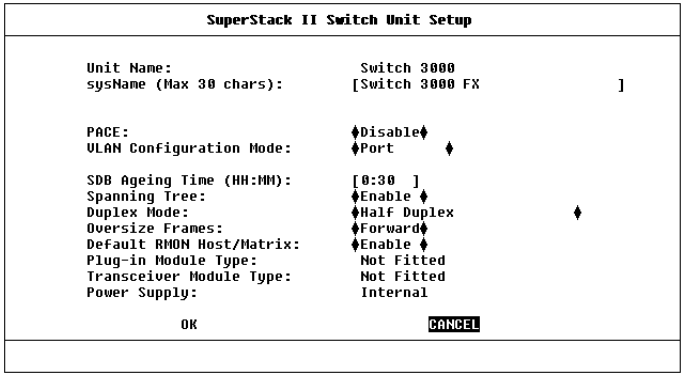

SuperStack II Switch Unit Setup
Unit Name: Switch 3000
sysName (Max 30 chars): [Switch 3000 FX]
PACE: ♦Disable♦
VLAN Configuration Mode: ♦Port ♦
SDB Ageing Time (HH:MM): [0:30]
Spanning Tree: ♦Enable ♦
Duplex Mode: ♦Half Duplex ♦
Oversize Frames: ♦Forward♦
Default RMON Host/Matrix: ♦Enable ♦
Plug-in Module Type: Not Fitted
Transceiver Module Type: Not Fitted
Power Supply: Internal
OK
CANCEL

Figure 5-13 Unit Setup screen

Configuring STP on the Switch

CAUTION: *You should not configure any STP parameters unless you have considerable knowledge and experience with STP.*

Configuring the STP Parameters of VLANs

The Switch has a completely separate STP system for each VLAN that you have specified. Each VLAN has its own Root Bridge, Root Ports, and BPDUs.

The VLAN STP screen allows you to set up and manage an STP system for each VLAN on the Switch. To access the VLAN STP screen:

1. From the Main Menu, select SWITCH MANAGEMENT. The Switch Management screen is displayed.
2. In the Management Level field, choose VLAN.
3. Choose the STP button. The VLAN STP screen is displayed, as shown in Figure 5-14.

The VLAN STP screen shows the following:

VLAN ID *1 / 2 / 3 ... 13 / 14 / 15* This field allows you to specify the VLAN to be configured.

If you are using STP, you cannot use VLAN 16. Also, if you are using AutoSelect VLAN Mode, you cannot use VLAN 15. In these cases, the relevant VLANs are used internally by the Switch and are therefore not available.

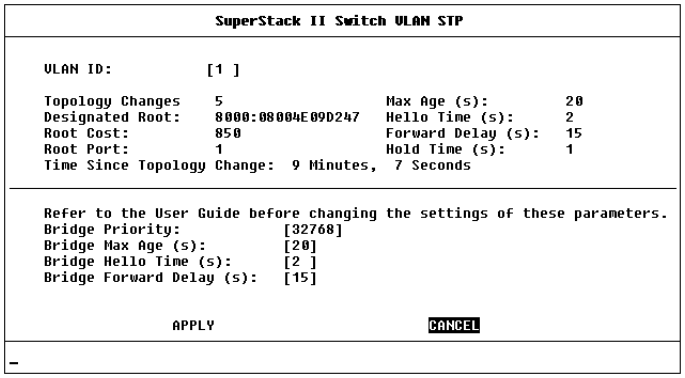

SuperStack II Switch VLAN STP
VLAN ID: [1]
Topology Changes 5
Designated Root: 8000:08004E09D247
Root Cost: 850
Root Port: 1
Time Since Topology Change: 9 Minutes, 7 Seconds
Max Age (s): 20
Hello Time (s): 2
Forward Delay (s): 15
Hold Time (s): 1
Refer to the User Guide before changing the settings of these parameters.
Bridge Priority: [32768]
Bridge Max Age (s): [20]
Bridge Hello Time (s): [2]
Bridge Forward Delay (s): [15]
APPLY
CANCEL

Figure 5-14 VLAN STP screen

Topology Changes This read-only field shows the number of network topology changes that have occurred in the current VLAN.

Max Age *6 ... 40* This read-only field shows the time (in seconds) that the Switch waits before trying to re-configure the network. If the Switch has not received a BPDU within the time specified in this field, it will try to re-configure the network topology.

Designated Root This read-only field shows the Bridge Identifier of the designated Root Bridge.

Hello Time *1 ... 10* This read-only field shows the time delay (in seconds) between the transmission of BPDUs from the Switch.

Root Cost This read-only field shows the path cost from the Switch to the Root Bridge.

Forward Delay *4 ... 30* This read-only field shows the time (in seconds) that the ports on the Switch spend in the listening and learning states. For more information about these states, refer to "Configuring the STP Parameters of Ports" on page 5-20.

Root Port This read-only field shows the Root Port of the Switch.

Hold Time This read-only field shows the shortest time interval (in seconds) allowed between the transmission of BPDUs.

Time Since Topology Change This read-only field shows the time interval since the last topology change was detected.

Bridge Priority *0 ... 65535* This field allows you to specify the priority of the Switch. By changing the priority of the Switch, you can make it more or less likely to become the Root Bridge. The lower the number, the more likely it is that the bridge will be the Root Bridge. The default setting for this field is 32768.

Bridge Max Age *6 ... 40* This field allows you to specify the time (in seconds) that the Switch waits before trying to re-configure the network when it is the Root Bridge. If the Switch has not received a BPDU within the time specified in this field, it will try to re-configure the STP topology. The default setting for this field is 20 seconds.

The time must be greater than, or equal to 2 x (Hello Time + 1) and less than, or equal to, 2 x (Forward Delay – 1).

Bridge Hello Time *1 ... 10* This field allows you to specify the time delay (in seconds) between the transmission of BPDUs from the Switch when it is the Root Bridge. The default setting for this field is 2 seconds.

Bridge Forward Delay *4 ... 30* This field allows you to specify the time (in seconds) that the ports on the Switch spend in the listening and learning states when the Switch is the Root Bridge. The default setting is 15 seconds. For more information about these states, refer to "Configuring the STP Parameters of Ports" on page 5-20.

APPLY This button applies any changes to the STP system.

Configuring the STP Parameters of Ports

The Port STP screen allows you to set up and manage the STP parameters of each port on the Switch. To access the Port STP screen:

1. From the Main Menu, select SWITCH MANAGEMENT. The Switch Management screen is displayed.
2. In the Management Level field, choose Port.
3. In the Port ID field, enter the ID of the port to be configured.
4. Choose the STP button. The Port STP screen is displayed, as shown in Figure 5-15.

The Port STP screen shows the following:

Port ID *1 / 2 / 3 ... 6 / 7 / 8* This read-only field shows the ID of the port to be configured.

STP State *Disabled / Listening / Blocking / Learning / Forwarding* This read-only field shows the current state of the port:

- *Disabled* — A port in this state does not forward packets, and does not participate in STP operation.
- *Listening* — A port in this state is preparing to forward packets, but has temporarily blocked to prevent a loop. During the Listening state, BPDUs are transmitted, received and processed.
- *Blocking* — A port in this state does not forward packets to prevent more than one active path existing on the network. The port is included in STP calculations, and BPDUs can be transmitted, received and processed.

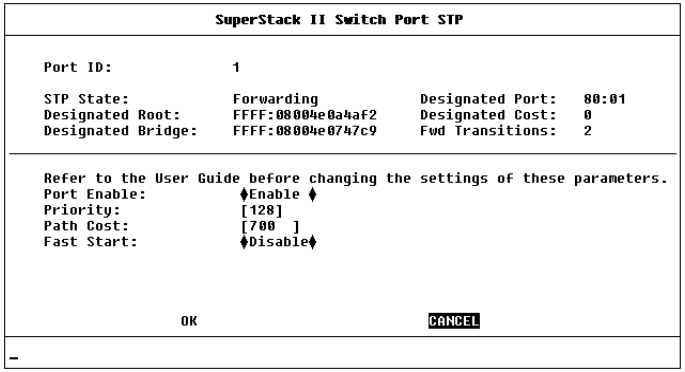


Figure 5-15 Port STP screen

- *Learning* — A port in this state is preparing to forward packets, but has temporarily blocked to prevent a loop. During the Learning state, the Switch learns the addresses of all error-free packets. The port is included in STP calculations, and BPDUs can be transmitted, received and processed.
- *Forwarding* — A port in this state can forward packets. BPDUs can also be received and processed.

Designated Port This read-only field shows the ID of the Designated Bridge Port for the current port's segment.

Designated Root This read-only field shows the Bridge Identifier of the Root Bridge.

Designated Cost This read-only field shows the path cost from the Root Bridge to the Designated Bridge Port for the current port's segment.

Designated Bridge This read-only field shows the Bridge Identifier of the Designated Bridge for the current port's segment.

Fwd Transitions This read-only field shows the number of times that the current port has transitioned from the Learning state to the Forwarding state.

Port Enable *Enable / Disable* This field allows you to enable or disable the current port.

Priority *0 ... 255* This field allows you to specify the priority of the port. By changing the priority of the port, you can make it more or less likely to become the Root Port. The lower the number, the more likely it is that the port will be the Root Port. The default setting for this field is 128.

Path Cost *0 ... 65535* This field allows you to specify the path cost of the port.

The Switch automatically assigns the default path costs shown in Table 5-1 on page 5-14. If you specify a new path cost in this field, this automatic system is disabled, and you can only re-enable it by initializing the Switch.

Fast Start *Enable / Disable* This field allows you to specify whether the port goes directly to the Forwarding state when a device is connected to it. Set this field to Enable if the port is directly connected to an endstation. The default setting for this field is Disable.

CAUTION: *If you set the Fast Start field to Enable when the port is connected to multiple endstations, loops may occur in your network.*

RMON

Using the RMON (Remote Monitoring) capabilities of your Switch allows network administrators to improve their efficiency and reduce the load on their network.

The following sections explain more about the RMON concept and the RMON features supported by the Switch.

You can only use the RMON features of the Switch if you have an RMON management application, such as the RMON application supplied with 3Com's Transcend Enterprise Manager.

What is RMON?

RMON is the common abbreviation for the Remote Monitoring MIB (Management Information Base), a system defined by the IETF documents RFC 1271 and RFC 1757, which allows you to monitor LANs remotely.

A typical RMON setup consists of two components:

- **The RMON probe** — An intelligent, remotely-controlled device or software agent that continually collects statistics about a LAN segment or VLAN, and transfers the information to a management workstation on request or when a pre-defined threshold is crossed.
- **The management workstation** — Communicates with the RMON probe and collects the statistics from it. The workstation does not have to be on the same network as the probe and can manage the probe by in-band or out-of-band connections.

About the RMON Groups

The IETF define nine groups of Ethernet RMON statistics. This section describes these groups, and details how they can be used.

Statistics

The Statistics group provides traffic and error statistics showing packets, bytes, broadcasts, multicasts and errors on a LAN segment or VLAN.

Information from the Statistics group is used to detect changes in traffic and error patterns in critical areas of your network.

History

The History group provides historical views of network performance by taking periodic samples of the counters supplied by the Statistics group. The group features user-defined sample intervals and bucket counters for complete customization of trend analysis.

The group is useful for analysis of traffic patterns and trends on a LAN segment or VLAN, and to establish baseline information indicating normal operating parameters.

Alarms

The Alarms group provides a versatile, general mechanism for setting thresholds and sampling intervals to generate events on any RMON variable. Both rising and falling thresholds are supported, and thresholds can be on the absolute value of a variable or its delta value. In addition, alarm thresholds may be autocalibrated or set manually.

Alarms are used to inform you of a network performance problem and they can trigger automated action responses through the Events group.

Hosts

The Hosts group specifies a table of traffic and error statistics for each host on a LAN segment or VLAN. Statistics include packets sent and received, octets sent and received, as well as broadcasts, multicasts, and error packets sent.

The group supplies a simple discovery mechanism listing all hosts that have transmitted. The next group, Hosts Top N, requires implementation of the Hosts group.

Hosts Top N

The Hosts Top N group extends the Hosts table by providing sorted host statistics, such as the top 20 nodes sending packets or an ordered list of all nodes according to the errors they sent over the last 24 hours.

Matrix

The Matrix group shows the amount of traffic and number of errors between pairs of devices on a LAN segment or VLAN. For each pair, the Matrix group maintains counters of the number of packets, number of octets, and error packets between the nodes.

The conversation matrix helps you to examine network statistics in more detail to discover who is talking to whom or if a particular PC is producing more errors when communicating with its file server, for example. Combined with Hosts Top N, this allows you to view the busiest hosts and their primary conversation partners.

Filter

The Filter group provides a mechanism to instruct the RMON probe to capture packets that match a specific criterion or condition.

Capture

The Capture group allows you to create capture buffers on the probe that can be requested and uploaded to the management workstation for decoding and presentation.

Events

The Events group provides you with the ability to create entries in an event log and/or send SNMP traps to the management workstation. Events can originate from a crossed threshold on any RMON variable. In addition to the standard five traps required by SNMP (link up, link down, warm start, cold start, and authentication failure), RMON adds two more: rising threshold and falling threshold.

Effective use of the Events group saves you time; rather than having to watch real-time graphs for important occurrences, you can depend on the Event group for notification. Through the SNMP traps, events can trigger other actions providing a mechanism for an automated response to certain occurrences.

Benefits of RMON

Using the RMON features of your Switch has three main advantages:

- **RMON improves your efficiency**

  Using RMON probes allows you to remain at one workstation and collect information from widely dispersed LAN segments or VLANs. This means that the time taken to reach a problem site, set up equipment, and begin collecting information is largely eliminated.

- **RMON allows proactive management**

  If they are configured correctly, RMON probes deliver information before problems occur. This means that you can take action before they impact on users. In addition, probes record the behavior of your network, so that you can analyze the causes of problems.

- **RMON reduces the traffic load**

  Traditional network management involves a management workstation polling network devices at regular intervals to gather statistics and identify problems or trends. As network sizes and traffic levels grow, this approach places a strain on the management workstation and also generates large amounts of traffic.

  An RMON probe, however, autonomously looks at the network on behalf of the management workstation without affecting the characteristics and performance of the network. The probe reports by exception, which means that it only informs the management workstation when the network has entered an abnormal state.

RMON and the Switch

RMON requires one probe per LAN segment, and stand-alone RMON probes have traditionally been expensive. Therefore, 3Com's approach has been to build an inexpensive RMON probe into the SmartAgent of each Switch. This allows RMON to be widely deployed around the network without costing more than traditional network management.

A problem with stand-alone RMON probes is that they are passive; able to monitor and report, but nothing more. Placing probe functionality inside the network device allows integration of RMON with normal device management to allow proactive management.

For example, statistics can be related to individual ports and the Switch can take autonomous actions such as disabling a port (temporarily or permanently) if errors on that port exceed a pre-defined threshold. Also, since a probe needs to be able to see all traffic, a stand-alone probe has to be attached to a non-secure port. Implementing RMON in the Switch means all ports can have security features enabled.

RMON Features of the Switch

Table 5-2 details the RMON support provided by the Switch.

Table 5-2 RMON support supplied by the Switch

RMON Group	Support supplied by the Switch
Statistics	A new or initialized Switch has one Statistics session per port/VLAN.
History	A new or initialized Switch has three History sessions on each 100BASE-FX port, the 100BASE-TX port and the Default VLAN: ■ 60-second intervals, 120 historical samples stored ■ 30-second intervals, 120 historical samples stored ■ 30-minute intervals, 96 historical samples stored
Alarms	Although up to 700 alarms can be defined for the Switch, a new or initialized Switch has four alarms defined for each port: ■ Bandwidth used ■ Broadcast bandwidth used ■ Percentage of packets forwarded ■ Errors per 10,000 packets You can modify these alarms using an RMON management application, but you cannot create or delete them. For more information about the alarms setup on the Switch, refer to "About Alarm Actions" on page 5-27 and "About Default Alarm Settings" on page 5-28.

Table 5-2 RMON support supplied by the Switch

RMON Group	Support supplied by the Switch
Hosts	Although Hosts is supported by the Switch, there are no Hosts sessions defined on a new or initialized Switch by default. You can specify that a Hosts session is defined on the Default VLAN; for more information, refer to "Setting Up the Switch Unit" on page 4-9.
Hosts Top N	Although Hosts Top N is supported by the Switch, there are no Hosts Top N sessions defined on a new or initialized Switch.
Matrix	Although Matrix is supported by the Switch, there are no Matrix sessions defined on a new or initialized Switch by default. You can specify that a Matrix session is defined on the Default VLAN; for more information, refer to "Setting Up the Switch Unit" on page 4-9.
Filter	The Filter group is not presently supported by the Switch.
Capture	The Capture group is not presently supported by the Switch.
Events	A new or initialized Switch has events defined for use with the default alarm system. Refer to "About Default Alarm Settings" on page 5-28 for more information.

When using the RMON features of the Switch, you should note the following:

- After the default sessions are created, they have no special status. You can delete or change them as required.
- The Switch 3000 FX can forward a very large volume of packets per second. The Statistics RMON group is able to monitor every packet, but the other groups sample a maximum of 6000 packets a second.
- The greater the number of RMON sessions, the greater the burden on the management resources of the Switch; however, the forwarding performance of the Switch is not affected.

About Alarm Actions

You can define up to 700 alarms for the Switch. The actions that you can define for each alarm are shown in Table 5-3.

Table 5-3 Alarm Actions

Action	High Threshold	Low Threshold
No action.		
Notify only.	Send Trap.	
Notify and blip port.	Send Trap. Block broadcast and multicast traffic on the port for 5 seconds.	
Notify and disable port.	Send Trap. Turn port off.	
Notify and enable port.		Send Trap. Turn port on.
Blip port.	Block broadcast and multicast traffic on the port for 5 seconds.	
Disable port.	Turn port off.	
Enable port.		Turn port on.
Notify and move resilient port.	Send Trap. If port is the main port of a resilient link pair then move to standby.	
Notify and blip device.	Send Trap. Block broadcast and multicast traffic on all ports for 5 seconds.	
Notify and disable device.	Send trap. Turn all ports on device off.	
Notify and enable device.		Send Trap. Turn ports back to original state.
Blip device.	Block broadcast and multicast traffic on all ports for 5 seconds.	
Disable device.	Turn all ports on device off.	
Re-enable device.		Turn ports back to original state.

About Default Alarm Settings

A new or initialized Switch has four alarms defined for each port:

- Bandwidth used
- Broadcast bandwidth used
- Percentage of packets forwarded
- Errors per 10,000 packets

The default values and actions for each of these alarms are given in Table 5-4.

Table 5-4 Initial settings for the default alarms

Statistic	High Threshold	Low Threshold Recovery	Samples per average	Period
Bandwidth used	Value: 85% No action	Value: 50% No action	4	60 seconds
Broadcast bandwidth used	Value: 20% Notify and blip	Value: 10% No action	4	20 seconds
Percentage of packets forwarded	Value: 85% No action	Value: 50% No action	4	60 seconds
Errors per 10,000 packets	Value: 200 Notify	Value: 100 No action	4	60 seconds

About the Audit Log

The Switch keeps an audit log of all management user sessions, providing a record of changes to any MIB including the RMON MIB. The log can only be read by users at the *security* access level using an SNMP Network Manager.

Each entry in the log contains information in the following order:

- Entry number
- Timestamp
- User ID
- Item ID (including qualifier)
- New value of item

There is a limit of 16 records on the number of changes stored. The oldest records are overwritten first.

6 STATUS MONITORING AND STATISTICS

This chapter describes how to view the current operating status of the Switch, how to display any error information in a fault log and how to carry out a remote poll to check the response of another network device.

It also describes the Statistics screens for the Switch, and advises you on actions to take if you see unexpected values for the statistics. Please note however, that as all networks are different, any actions listed are only suggestions.

Viewing statistics on a regular basis allows you to see how well your network is performing. If you keep simple daily records, you will see trends emerging and notice problems arising before they cause major network faults. This way, statistics can help you get the best out of your network.

Summary Statistics

With the Switch Management screen displayed, choose the management level *Unit*, then select the STATISTICS button. The Summary Statistics screen is displayed, as shown in Figure 6-1.

The Summary Statistics screen lists values for the current counter against every port on the Switch and it is refreshed approximately every 2 seconds. Once values have reached approximately 4,000,000,000 they are reset to zero.

To view values for a particular counter, select the first button displayed at the foot of the Summary Statistics screen. Pressing [Space] toggles through the available counters and as soon as you move away from the button, the screen is refreshed to show values for that counter.

FRAMES RECEIVED Displays the total number of frames that have been received by the current port, including fragments and frames with errors.

FRAMES TRANSMITTED Displays the total number of frames successfully transmitted by the current port.

FRAMES FORWARDED Displays the total number of frames that were received by the current port and forwarded to other ports.

FRAMES FILTERED Displays the total number of frames that were filtered because the destination station was on the same segment (port) as the source station.

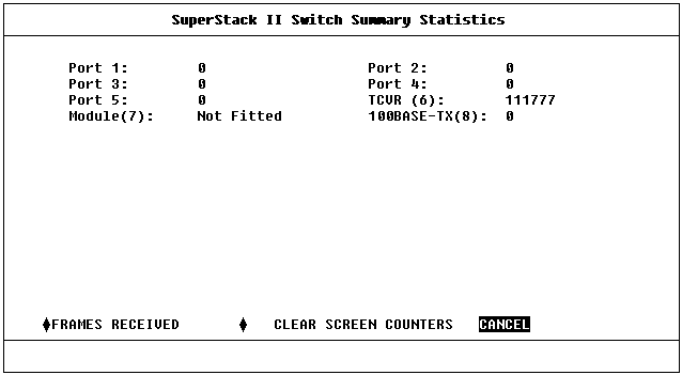


Figure 6-1 Summary Statistics screen

MULTI/BROADCAST (RX) Displays the total number of frames received by the current port that are addressed to a multicast or broadcast address.

MULTI/BROADCAST (TX) Displays the total number of frames transmitted by the current port that are addressed to a multicast or broadcast address.

ERRORS Displays the total number of errors that have occurred on the current port. Refer to the field description for Errors on page 6-5.

CLEAR SCREEN COUNTERS Use this button to set all counters shown on the screen to zero. Use this button for analysis if you wish to see changes in counters over a short period of time. This button does not clear the counters on the device.

Port Statistics

With the Switch Management screen displayed, choose the management level *port*, then select the STATISTICS button. The Port Statistics screen is displayed as shown in Figure 6-2.

As well as showing statistics for the port, the Port Statistics screen allows you access to traffic and error counter screens.

If the port is an ATM OC-3c Module port, the ATM Port Statistics screen is displayed. For more information, refer to the "SuperStack® II Switch ATM OC-3c Module User Guide".

The Port Statistics screen shows the following:

Port ID The ID of the port you are currently managing.

Bandwidth Used This counter provides a running average of the bandwidth used by the port, expressed as a percentage of the maximum bandwidth available for the port. A sampling period of 1 minute is used. The value gives an indication of the general traffic level of the network. A high utilization for single endstation segments is an indication that your network is operating efficiently. However, if multiple endstations are connected to this port and you see values of around 40% you should reconsider the topology of your network because each user will see degraded network performance.

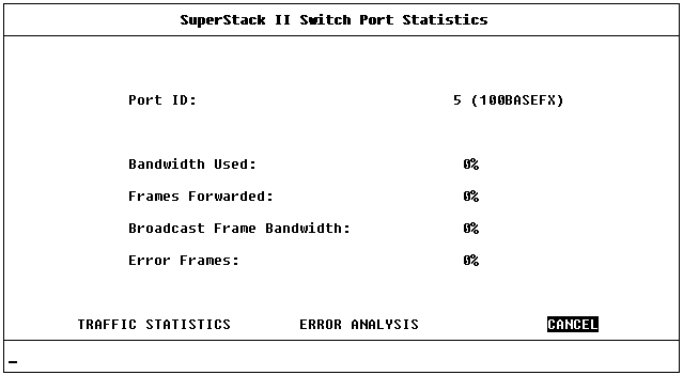


Figure 6-2 Port Statistics screen

Frames Forwarded This counter provides a running average of the proportion of frames received by the port that are forwarded, expressed as a percentage of all frames received by the port. A sampling period of 1 minute is used.

Broadcast Frame Bandwidth This counter provides a running average of the broadcast frame bandwidth used by the port, expressed as a percentage of the maximum bandwidth available for the port. A sampling period of 5 seconds is used.

Error Frames This counter provides a running average of the number of errors per 10,000 frames received by the port, expressed as a percentage. Refer to the field description for Errors on page 6-5.

TRAFFIC STATISTICS Select this button to access traffic counters for the port.

ERROR ANALYSIS Select this button to access error counters for the port.

Port Traffic Statistics

With the Port Statistics screen displayed, select the TRAFFIC STATISTICS button. The Port Traffic Statistics screen is displayed, as shown in Figure 6-3.

The Port Traffic Statistics screen shows the following:

Port ID The ID of the port you are currently managing.

Frames Received The number of valid frames received by the port, including fragments and frames with errors.

Frames Transmitted The number of frames that have been successfully transmitted by the port, including fragments and frames with errors.

Octets Received The number of octets received by the port. The calculation includes the MAC header and Cyclical Redundancy Check (CRC), but excludes preamble/Start-of-Frame-Delimiter (SFD). Octet counters are accurate to the nearest 256 octet boundary.

Octets Transmitted The number of octets transmitted by the port. The calculation includes the MAC header and CRC, but excludes preamble/SFD. Octet counters are accurate to the nearest 256 octet boundary.

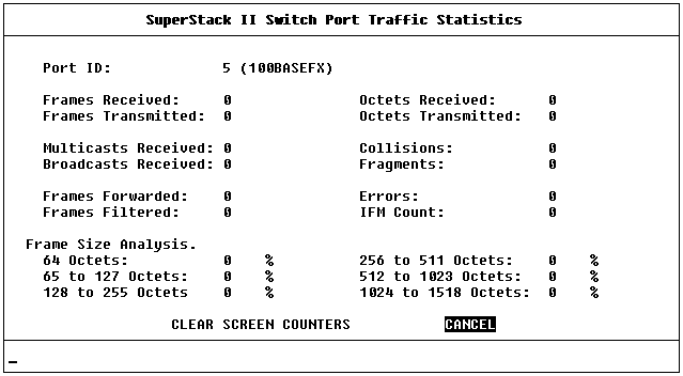


Figure 6-3 Port Traffic Statistics screen

Multicasts Received The number of frames successfully received that have a multicast destination address. This does not include frames directed to a broadcast address or frames received with errors.

Broadcasts Received The number of frames received that have a broadcast destination address. This does not include frames with errors.

Collisions An estimate of the total number of collisions that occurred when transmitting from the unit. Collisions are a normal part of Ethernet operation that occur when two devices attempt to transmit at the same time. A sudden sustained increase in the number of collisions may indicate a problem with a device or cabling on the network, particularly if this is not accompanied by an increase in general network traffic.

Fragments The total number of packets received that were not an integral number of octets in length or that had a bad Frame Check Sequence (FCS), and were less than 64 octets in length (excluding framing bits, but including FCS octets).

Frames Forwarded The total number of frames which were received by the port and forwarded to their destination address.

Frames Filtered The total number of frames that were filtered because the destination address was on the same segment (port) as the source station.

Errors The total number of errors which have occurred on this port. Errors can be one of the following:

- CRC Alignment Errors
- Short Events
- Long Frames
- Late Events
- Jabbers

The value shown should be a very small proportion of the total data traffic.

IFM Count The number of times Intelligent Flow Management (IFM) has had to operate to minimize packet loss.

Frame Size Analysis The number of frames of a specified length as a percentage of the total number of frames of between 64 and 1518 octets. This indicates the composition of frames in the network.

The frame size ranges are:

- 64 octets
- 65–127 octets
- 128–255 octets
- 256–511 octets
- 512–1023 octets
- 1024–1518 octets

The composition of frames on your network may help you to analyze the efficiency of your network layer protocol.

CLEAR SCREEN COUNTERS Select this button to set all counters shown on the screen to zero. It is useful for trend analysis if you wish to see changes in counters over a short period of time. This button does not clear the counters on the device or affect counters at the network management workstation.

Port Error Analysis

With the Port Statistics screen displayed, select the ERROR ANALYSIS button. The Port Error Analysis screen is displayed, as shown in Figure 6-4.

The Port Error Analysis screen shows the following:

Port ID The ID of the port you are currently managing.

CRC Align Errors This counter is incremented by one for each frame with a CRC (Cyclical Redundancy Check) error or an alignment error. A CRC occurs if a frame of valid length has an invalid CRC but does not have a framing error. It is likely that a bit has been corrupted in transmission. An alignment error occurs if a frame has a CRC error and does not have an integral number of octets. Alignment errors may be caused by a fault at the transmitting device.

Check cables and connections for damage. If this does not solve the problem, try changing the transceiver or adapter card of the device connected to the port at the source of the problem.

Short Events This counter is incremented by one for each carrier event whose duration is less than the short event maximum time. Short events are error frames smaller than the minimum size defined for Ethernet frames. They may indicate externally generated noise causing problems on the network. Check the cabling routing and re-route any cabling which may be affected by external noise sources.

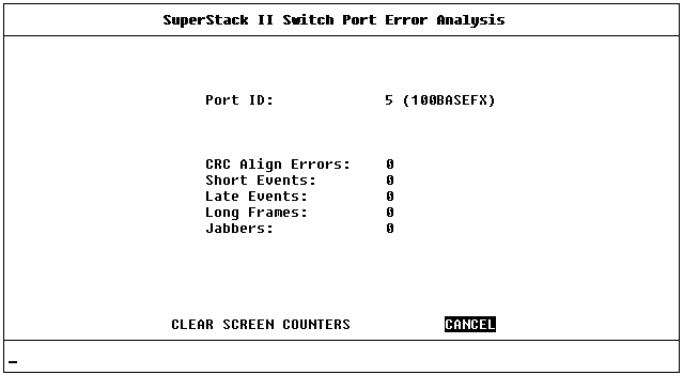


Figure 6-4 Switch Port Error Analysis screen

Late Events This counter is incremented by one each time a collision occurs after the valid packet minimum time. A late event is an out-of-window collision that may occur if your Ethernet LAN exceeds the maximum size as defined in the IEEE standard. A late event is also counted as a collision.

Long Frames This counter is incremented by one each time a frame is received whose octet count is greater than the maximum frame size but less than Jabber frame size. Long Frames are frames that exceed the maximum size defined for Ethernet frames (1518 octets). If you see a high number of long frames on your network, you should isolate the source of these frames and examine the transceiver or adapter card at the device. Some protocols may generate these frames.

Jabbers The total number of packets received that were longer than 8K octets (excluding framing bits, but including FCS octets).

CLEAR SCREEN COUNTERS Select this button to set all counters shown on the screen to zero. It is useful for trend analysis if you wish to see changes in counters over a short period of time. This button does not clear the counters on the device or affect counters at the network management workstation.

Status Monitoring

The status screen provides read-only information about the Switch. This information may be useful for your technical support representative if you have a problem.

To access the screen, from the Main Menu, select the STATUS option. The Status screen is displayed, as shown in Figure 6-5.

The Status screen shows the following:

System Up Time The time the unit has been running since the last reset or power-off/on cycle.

Number of Resets The total number of system resets since the Switch was first installed or initialized; either power on, manual reset or a watchdog expiry.

Last Reset Type *Other* / *Command* / *Watchdog* / *Power-reset* / *System-error* This field indicates the cause of the last reset. It may be due to management command, watchdog timeout expiry, power interruption, a manual reset or a system error.

Hardware Version The hardware version number of the Switch.

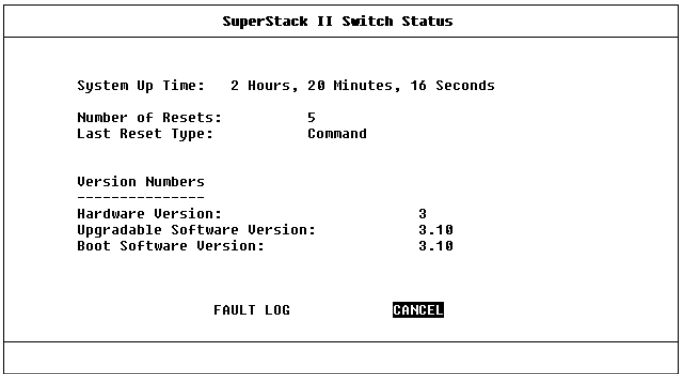


Figure 6-5 Status screen

Upgradable Software Version The version number of the agent software image stored in Flash EPROM. This version number is automatically updated when you download new software.

Boot Software Version This is the version number of the Boot software stored on the Switch.

FAULT LOG Select this button to display the Switch Fault Log, described in the next section.

Fault Log

The Fault Log displays read-only information about the Switch which is updated whenever an abnormal condition is detected. This information is for internal 3Com use only. You may be asked to quote this information if reporting a fault to your supplier.

With the Status screen displayed, select the FAULT LOG button. The Fault Log is screen is displayed, as shown in Figure 6-6.

The Fault Log screen shows the following:

Reset Count The number of resets recorded at the time of the fault.

Time (seconds) The time elapsed since the last reset when the fault occurred.

Area This information may be used for fault diagnosis by your technical support representative.

Fault Number The hexadecimal number in this field indicates the type of fault. You should note this number and contact your technical support representative for advice.

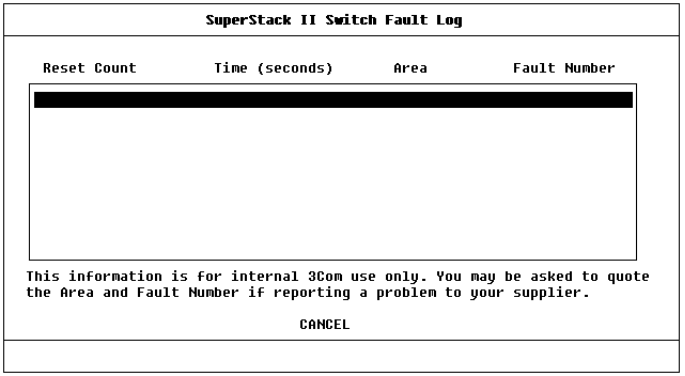

SuperStack II Switch Fault Log
Reset Count
Time (seconds)
Area
Fault Number
This information is for internal 3Com use only. You may be asked to quote the Area and Fault Number if reporting a problem to your supplier.
CANCEL

Figure 6-6 Fault Log screen

Remote Polling

The Remote Poll screen allows you to send a single frame to a remote device to see if that device is responding. This can help to locate the source of a network problem. It is also particularly helpful in locating devices that support IP, IPX and ping but are not manageable by SNMP.

To poll a device:

1. From the Main Menu, select Remote Poll. The Remote Poll screen is displayed, as shown in Figure 6-7.
2. In the Target Address field, enter the IP or IPX address of the device you want to poll.
3. Select the POLL button at the foot of the screen.

When the poll is complete, the Round Trip Time field shows the interval in milliseconds between sending the frame to the target device and receiving a response at the Switch. If the target device does not respond after approximately 10 seconds, this field displays *no reply*.

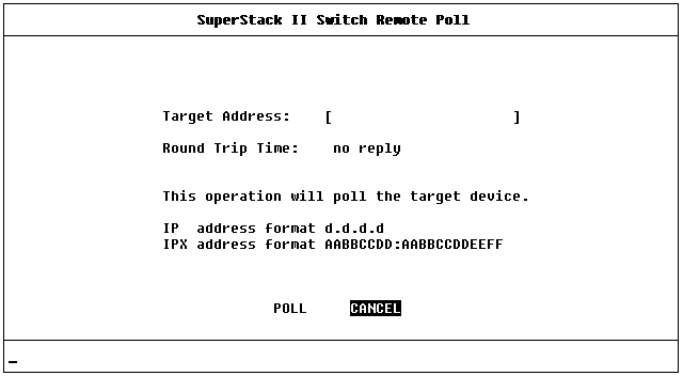
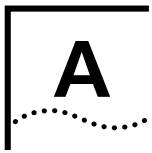


Figure 6-7 Remote Poll screen



SAFETY INFORMATION

Before carrying out any installation or removal of components, or any maintenance procedures on the Switch, you must read the following safety information.

Important Safety Information

WARNING: *Warnings contain directions that you must follow for your personal safety. Follow all instructions carefully.*

Please read the following safety information thoroughly before installing the Switch.

- Installation and removal of the unit must be carried out by qualified personnel only.
- If installing the Switch unit in a stack with SuperStack® II Hub units, the Switch unit must be installed below the narrower Hub units.
- This unit must be earthed.
- Connect the unit to an earthed power supply to ensure compliance with European safety standards.
- The power cord set must be approved for the country where it will be used.
- The appliance coupler, that is, the connector to the device itself and not the wall plug, must have a configuration for mating with an EN60320/IEC320 appliance inlet.
- For U.S.A. and Canada:
  - The cord set must be UL-approved and CSA certified.
  - The minimum specification for the flexible cord are:

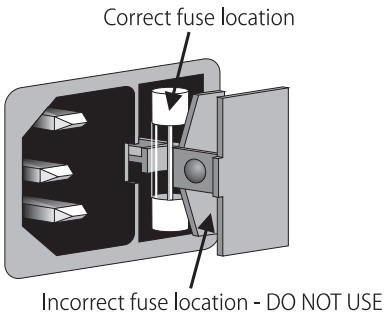
    No. 18 AWG
    Type SV or SJ
    3-conductor
  - The cord set must have a rated current capacity of at least 10A.
  - The attachment plug must be an earth-grounding type with a NEMA 5-15P (15A, 125V) or NEMA 6-15P (15A, 250V) configuration.
- For Denmark:
  - The supply plug must comply with section 107-2-D1, standard sheet DK2-1a or DK2-5a.
- For Switzerland:
  - The supply plug must comply with SEV/ASE 1011.

- It is essential that the mains socket outlet is installed near to the unit and is accessible. You can only disconnect the unit by removing the appliance coupler from the unit.
- If the power supply plug is unsuitable and you have to replace it, you may find other codings for the respective connections. Connect the power supply wires from the unit according to the following scheme:
- Brown wire to the Live (Line) plug terminal which may be marked with the letter L or colored red.
- Blue wire to the Neutral plug terminal which may be marked with the letter N or colored black.
- Yellow/green wire to the Earth (Ground) plug terminal which may be marked with the letter E, or the earth symbol or colored green/yellow.
- This unit operates under SELV conditions (Safety Extra Low Voltage) according to IEC 950, the conditions of which are maintained only if the equipment to which it is connected is also operational under SELV.
- Under no circumstances should the unit be connected to an A.C. outlet (power supply) without an Earth (Ground) connection.
- To comply with European safety standards, a spare fuse must not be fitted to the appliance inlet. Only fuses of the same manufacturer, make and type should be used with the unit.
- Ensure that the power supply lead is disconnected before opening the IEC connector fuse cover or removing the cover of the unit.
- France and Peru only:
  - This unit cannot be powered from IT (impedance à la terre) supplies. If your supplies are of the IT type, this unit should be powered by 230V (2P+T) via an isolation transformer ratio 1:1, with the secondary connection point labelled Neutral, connected directly to Earth (Ground).
- U.K. only:
  - The Switch is covered by Oftel General Approval, NS/G/12345/J/100003, for indirect connection to a public telecommunications system. This can only be achieved using the console port on the unit and an approved modem.
- Do not remove the Plug-in Module or Transceiver Module blanking plate with the power still connected.

Power Supply and Fuse

The unit automatically adjusts to the supply voltage. The fuse is suitable for both 110V A.C. and 220–240V A.C. operation.

WARNING: *Ensure that the power is disconnected before opening the fuse holder cover.*



To change the fuse, release the fuse holder by gently levering a small screwdriver under the fuse holder catch. Only 5A Time Delay (anti-surge) fuses of the same type and manufacture as the original should be used.

Sockets for Redundant Power System (RPS)

Only connect a 3Com Redundant Power System to this socket. For details, follow the installation instructions in the manuals accompanying the Redundant Power System.

RJ45 Ports

WARNING: *The RJ45 ports are shielded RJ45 data sockets. They cannot be used as telephone sockets. Only connect RJ45 data connectors to these sockets.*

Either shielded or unshielded data cables with shielded or unshielded jacks can be connected to these data sockets.

Fiber Ports

WARNING: Optical safety

Under normal viewing conditions, there is no hazard from the fiber Transmit LED. It is recommended however, that the LED is not viewed through any magnifying device whilst it is powered on. It is advisable that the fiber Tx port and fiber cable ends are never viewed directly when powered-on.

L'information de Sécurité Importante

AVERTISSEMENT: *Les avertissements contiennent les directions que vous devez suivre pour votre sécurité personnelle. Suivez toutes les directives avec soin.*

Veuillez lire à fond l'information de la sécurité suivante avant d'installer le Switch.

- L'installation et l'enlèvement de l'unité doivent être faits seulement par le personnel qualifié.
- Si vous entassez l'unité Switch avec les unités SuperStack II Hub, l'unité Switch doit être installée en dessous des unités Hub plus étroites.
- Cette unité doit être mise à la terre.
- Brancher l'unité à une source de courant mise à la terre pour assurer la conformité aux normes de sécurité européennes.
- La cordon d'alimentation surmoulé doit être approuvé pour le pays auquel il sera utilisé.
- Le socle de connecteur, c'est-à-dire, le connecteur à l'appareil lui-même et non pas la prise murale, doit avoir une configuration pour le branchement avec une admission d'appareil EN60320/IEC320.
- Pour USA et le Canada:
  - Le cordon surmoulé doit être UL Certifié et CSA Certifié.
  - Les spécifications minimales pour le cordon souple sont:

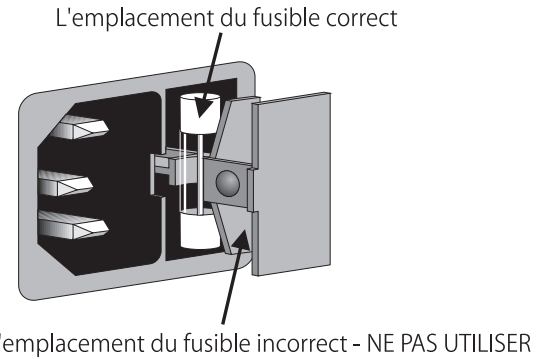
    No. 18 AWG
    Type SV ou SJ
    3-conducteur
  - Le cordon surmoulé doit avoir une capacité de courant calculée au moins de 10A.
  - La fiche de fixation doit être un type mis à la terre avec une configuration NEMA 5-15P (15A, 125V) ou NEMA 6-15P (15A, 250V).
- C'est essentiel que le socle soit installé près de l'unité et soit accessible. Vous pouvez seulement débrancher l'unité en enlevant la fiche d'alimentation de la prise de courant.
- Cette unité marche sous les conditions SELV (Safety Extra Low Voltage) conformément à IEC950, ces conditions sont maintenues seulement si le matériel auquel elle est branchée, est aussi en exploitation sous SELV.
- L'unité ne devrait pas être branchée à une prise de courant C.A. (source de courant) sous aucun prétexte sans un branchement mis à la terre (mis à la masse).
- Pour conformer aux normes de sécurité européennes, un fusible de rechange ne doit pas être ajusté à l'admission d'appareil. Seulement les fusibles du même fabricant, construit, et type doivent être utilisés avec l'unité.

- Assurer que l'entrée de la source d'alimentation soit débranchée avant d'ouvrir le couvercle de fusible du connecteur IEC ou d'enlever le couvercle de l'unité.
- Seulement Pour La France et Le Pérou:
  - Cette unité ne peut pas être mise en marche des sources de courant IT (Impédance à la terre). Si vos sources de courant sont de type IT, cette unité doit être alimentée par 230V (2P+T) via un rapport de transformation d'isolation de 1:1, avec un point de connexion secondaire étiqueté Neutre, branché directement à la Terre (à la Masse).
- Ne pas enlever le Module Plug-in ou la plaque d'occultation de module d'émetteur-récepteur avec la puissance encore branchée.

La Source de Courant et Le Fusible

L'unité s'ajuste automatiquement à la tension d'alimentation. Le fusible est convenable aux deux opérations 110 V C.A. et 220-240 V C.A.

AVERTISSEMENT: *Assurer que l'alimentation soit débranchée avant d'ouvrir le couvercle du contenant du fusible.*



Pour changer le fusible, dégager le contenant du fusible en mettant doucement un petit tournevis sous l'arrêt de contenant du fusible. Seulement les fusibles de types 5A anti-transitoires du même type et fabricant que l'original doivent être utilisés.

Socle Pour Alimentation Multiple

Brancher seulement une alimentation multiple de 3Com à cet socle. Suivre pour les détails les directives de l'installation dans le manuel qui accompagne l'alimentation multiple.

Les Ports RJ45

AVERTISSEMENT: *Ceux-ci sont les prises de courant de données RJ45 protégées. Ils ne peuvent pas être utilisés comme prises de courant téléphoniques. Brancher seulement les connecteurs RJ45 de données à ces prises de courant.*

Les câbles de données blindés ou non blindés, avec les jacks blindés ou non blindés, l'un ou l'autre, peuvent être branchés à ces prises de courant de données.

Les Ports Fibre

AVERTISSEMENT: Sécurité sur le plan optique

Sous les conditions de visionnement ordinaires, il n'y a pas de danger à l'oeil à cause de la diode électroluminescente d'émission. C'est recommandé, cependant, que la diode électroluminescente ne soit pas examinée avec aucun appareil de grossissement pendant qu'elle est sous tension. C'est recommandé que le port de fibre Tx et les fins de câble du fibre ne soient jamais directement examinées pendant qu'ils soient sous tension.

Wichtige Sicherheitsinformationen

WARNUNG: *Warnungen enthalten Anweisungen, die zur eigenen Sicherheit unbedingt zu beachten sind. Bitte befolgen Sie alle Anweisungen sorgfältig und genau.*

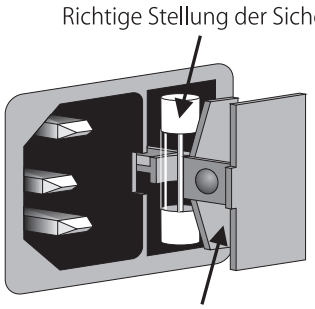
Bitte unbedingt vor dem Einbauen des Switch Einheit die folgenden Sicherheitsanweisungen durchlesen.

- Ein- und Ausbau des Gerätes ist nur von Fachpersonal vorzunehmen.
- Wenn die Switch Einheit in einer Stapel mit anderen SuperStack II Hub Einheiten eingebaut werden soll, muß die Switch Einheit unter die schmaleren Hub Einheiten eingebaut werden.
- Dieses Gerät muß geerdet sein.
- Das Gerät an geerdete Stromversorgung anschließen, um eine Übereinstimmung mit den europäischen Sicherheitsbestimmungen zu gewährleisten.
- Der Anschlußkabelsatz muß mit den Bestimmungen des Landes übereinstimmen, in dem er verwendet werden soll.
- Die Anordnung der Gerätsteckvorrichtung, d.h. die Steckverbindung am Gerät selbst im Gegensatz zum Wandstecker, muß in den EN60320/IEC320 Zuführungsstecker am Gerät passen.
- Es ist wichtig, daß der Netzstecker sich in unmittelbarer Nähe zum Gerät befindet und leicht erreichbar ist. Das Gerät kann nur durch Herausziehen des Verbindungssteckers aus der Steckdose vom Stromnetz getrennt werden.
- Das Gerät wird mit Sicherheits-Kleinspannung nach IEC 950 (SELV = Safety Extra Low Voltage) betrieben. Angeschloßen werden können nur Geräte, die ebenfalls nach SELV betrieben werden.
- Das Gerät ist unter keinen Umständen an einen Wechselstrom (A.C.) Netzstecker anzuschließen ohne Erdungsleitung.
- Um Übereinstimmung mit den europäischen Sicherheitsnormen zu gewährleisten, darf am Zuführungstecker des Gerätes keine Ersatzsicherung angebracht werden. Nur Sicherungen der gleichen Herstellung und Marke sowie des gleichen Typs für das Gerät verwenden.
- Vorm Öffnen der Abdeckungsklappe der IEC Steckverbindungssicherung oder vorm Abnehmen der Gesamtabdeckung der Gerät sicherstellen, daß das Stromverbindungskabel vom Netzstrom getrennt ist.
- Die Austastplatten der Plug-in Module — oder Sendeempfänger-Module nicht entfernen, solange die Einheit ans Stromnetz angeschlossen ist.

Stromversorgung und Sicherung

Das Gerät stellt sich automatisch auf die Versorgungsspannung ein. Die Sicherung ist sowohl für 110V A.C. wie für 220-240V A.C. geeignet.

WARNUNG: *Vor dem Öffnen der Sicherungshalterung das Gerät vom Netzstrom trennen.*



Zum Auswechseln der Sicherung durch leichtes Heben mit einem kleinen Schraubenzieher die Abdeckungsklappe der Sicherungshalterung lösen. Sicherungen nur durch gleichen Typ und Wert wie die Originalsicherung ersetzen. Sicherung auswechseln und die Klappe der Sicherungshalterung wieder schließen.

Steckdose für Redundant Power System (RPS)

Nur ein 3Com Redundant Power System an diese Steckdose anschließen. Für weitere Angaben die genauen Einbauanweisungen im Handbuch zum Redundant Power System befolgen.

RJ45 Anschlußen

WARNUNG: *Hierbei handelt es sich um abgeschirmte RJ45 Datenbuchsen, die nicht als Telefonbuchsen verwendbar sind. Nur RJ45 Datensteckverbinder an diese Buchsen anschließen.*

Diese Datenstecker können entweder mit abgeschirmten oder unabgeschirmten Datenkabeln mit abgeschirmten oder unabgeschirmten Klinkensteckern verbunden werden.

Glasfaser Anschlußen

WARNUNG: Optische Sicherheit

Unter normalen Umständen geht von der übertragenden LED keine Gefahr für die Augen aus. Es wird aber empfohlen, die LED nicht durch Vergrößerungslinsen zu betrachten solange die Leuchtdiode unter Strom steht. Ebenso ist es ratsam den Glasfaser Tx Anschluß und die Enden der Glasfaserkabel nicht direkt zu betrachten solange diese unter Strom stehen.

B SCREEN ACCESS RIGHTS

The following table lists the rights assigned to each level of user for accessing and editing Switch screens via the VT100 interface.

All access rights are read-and-write unless otherwise stated.

Screen	Available to...
Logon	Monitor Manager Security
Main Menu	Monitor Manager Security
Switch Management	Monitor Manager Security
Port STP	Monitor *read-only* Manager Security
Port Statistics	Monitor Manager Security
Port Traffic Statistics	Monitor Manager Security
Port Error Analysis	Monitor Manager Security
Port Resilience	Monitor Manager Security
Port Setup	Monitor *read-only* Manager Security
Unit Statistics	Monitor Manager Security
Unit Database View	Monitor Manager Security
Unit Resilience	Monitor Manager Security
Unit Setup	Monitor *read-only* Manager Security

Screen	Available to...
VLAN STP	Monitor *read-only* Manager Security
VLAN Server	Monitor *read-only* Manager Security
VLAN Setup	Monitor *read-only* Manager Security
User Access Levels	Monitor Manager Security
Local Security	Security
Create User	Security
Delete Users	Security
Edit User	Monitor Manager Security
Status	Monitor Manager Security
Fault Log	Monitor Manager Security
Management Setup	Monitor *read-only* Manager Security
Trap Setup	Monitor *read-only* Manager Security
Console Port Setup	Monitor *read-only* Manager Security
Software Upgrade	Security
Initialize	Security
Reset	Manager Security
Remote Poll	Manager Security

C TROUBLE-SHOOTING

The following is a list of problems you may see when managing the Switch with suggested courses of corrective action to take. If you have a problem which is not listed here and you cannot solve it, contact your local technical support representative.

LEDs

Power LED does not light:

Check that the power cable is firmly connected to the device and to the supply outlet.

Check the unit fuse. For information on changing the fuse, refer to "Power Supply and Fuse" in Appendix A.

On powering-up, the MGMT LED lights yellow:

The unit has failed its Power On Self Test (POST) and you should contact your supplier for advice.

On powering-up, the MGMT LED flashes yellow:

The installed Plug-in Module has failed its Power On Self Test (POST). Try re-installing the Plug-in Module, ensuring it is correctly seated. If the problem persists, contact your supplier for advice.

The Plug-in Module Status LED lights yellow:

If the MGMT LED is flashing yellow, the Module has failed its Power On Self Test; refer to the previous advice. Otherwise, the Module's agent software is not installed correctly. Refer to the User Guide supplied with the Module.

The Plug-in Module Status LED flashes yellow:

The Module is not recognized. You may need to download a version of the Switch's management agent software that recognizes the Module (refer to "Upgrading Software" on page 4-28), or remove the Module. Contact your supplier for further advice.

A link is connected and yet the Status LED does not light:

Check that:

- All connections are secure
- Cables are free from damage
- The devices at both ends of the link are powered-up
- The connection uses cross-over cable if you are linking a 10BASE-T or 100BASE-TX port with a device which is MDIX-only

Using the VT100 Interface

The initial Main Banner screen does not display:

Check that your terminal or terminal emulator is correctly configured to operate as a VT100 terminal.

For console port access, you may need to press [Return] several times before the Main Banner appears.

Check the settings on your terminal or terminal emulator. The management facility's auto configuration works only with baud rates from 1200 to 19,200.

Screens are incorrectly displayed:

Check that your terminal or terminal emulator is correctly configured to operate as a VT100 terminal.

Check the settings on your terminal or terminal emulator. The management facility's autoconfiguration works only with baud rates from 1200 to 19,200.

Check that you are using a suitable font (for example, in HyperTerminal use the MS Line Draw font).

The SNMP Network Manager cannot access the device:

Check that the device's IP address, subnet mask and default router are correctly configured, and that the device has been reset. Check that the device's IP address is correctly recorded by the SNMP Network Manager (refer to the user documentation for the Network Manager).

The Telnet workstation cannot access the device:

Check the device's IP address, subnet mask and default router are correctly configured, and that the device has been reset. Ensure that you enter the IP address of the Switch correctly when invoking the Telnet facility.

Traps are not received by the SNMP Network Manager:

Check that the SNMP Network Manager's IP address and the community string are correctly configured.

The SNMP Network Manager or Telnet workstation can no longer access the device:

Check that Remote Telnet access or Community-SNMP access is enabled.

Check that the port through which you are trying to access the device has not been disabled, refer to "Setting Up the Switch Ports" on page 4-11. If it is enabled, check the connections and network cabling at the port.

Check that the port through which you are trying to access the device is in VLAN 1 (the Default VLAN). Refer to "Setting Up VLANs on the Switch" on page 5-8.

Try accessing the device through a different port. If you can now access the device, a problem with the original port is indicated. Re-examine the connections and cabling.

There may be a network problem preventing you accessing the device over the network. Try accessing the device through the console port.

You forget your password and cannot log in:

If you are not one of the default users (monitor, manager, security or admin), another user having *security* access level can log in, delete your user name, and create a new user name for you, with a new password.

Alternatively, another user having *security* access level can log in and initialize the device. This will return all configuration information, including passwords, to the initial values. In the case where no-one knows a password for a security level user, contact your supplier.

Using the Switch

You see network problems and the Packet LED is on continuously with constant collisions (refer to "Port Traffic Statistics" on page 6-4):

You are using PACE equipped devices and have the Interactive Access feature of PACE enabled at both ends of the link. Interactive Access must only be enabled at one end of the Switch–device link. Disabling Interactive Access for a Switch port is described in "Setting Up the Switch Ports" on page 4-11.

You have configured a Switch port so that it 'blips' when a broadcast storm occurs, but the port does not blip properly:

The broadcast storms are occurring such that the average broadcast bandwidth cannot drop below the Falling Threshold value. This means that the blip only occurs once.

Try changing the following attributes in the Broadcast Storm Control section of the Port Setup screen:

- Rising Action to disable port/notify
- Falling Action to event + enable

For more information, refer to "Setting Up the Switch Ports" on page 4-11.

You have added the Switch 3000 FX to an already busy network, and response times and traffic levels have increased:

You may have added a group of users to one of the Switch 3000 FX ports via a repeater or switch, and not turned off Intelligent Flow Management (IFM). Turn off IFM on any port that is connected to multiple devices. Refer to "Setting Up the Switch Ports" on page 4-11.

You have connected an endstation directly to the Switch and the endstation fails to boot correctly:

The Switch has STP enabled, and the endstation is booting before the STP initialization process is complete. Specify that the port has Fast Start enabled, and then reboot the endstation. For more information about specifying Fast Start for a port, refer to "Configuring the STP Parameters of Ports" on page 5-20.

The Switch keeps ageing out endstation entries in the Switch Database (SDB):

The Switch has STP enabled, and STP is instructing the Switch to age entries in the SDB faster because topology changes are occurring in the network.

1. Reduce the number of topology changes by enabling Fast Start for all ports which are directly connected to an endstation; refer to "Configuring the STP Parameters of Ports" on page 5-20.
2. Specify that the endstation entries are Non-ageing; refer to "Setting Up the Switch Database (SDB)" on page 4-15.
3. Consider disabling STP on the Switch, and using resilient links to provide network resilience; refer to "Enabling STP on the Switch" on page 5-17 and "Setting Up Resilient Links" on page 4-18.

You are trying to manage the Switch over a network which has STP, and you are losing contact with the management agent intermittently.

As shown in Figure C-1, there is a SuperStack II Switch unit (Switch A) between your management workstation and the Switch 3000 FX (Switch B). You have configured more than one VLAN on both Switch units, and there is a parallel STP path for each VLAN between the Switch units.

When Switch B transmits BPDUs across a VLAN other than VLAN 1, Switch A learns the MAC address of Switch B through the port on that VLAN. The management agent of Switch B is only accessible through VLAN 1, and so your management workstation cannot communicate with Switch B until it transmits BPDUs across VLAN 1. When that occurs, Switch A learns the MAC address of Switch B through the port on VLAN 1.

To avoid this situation, we recommend that you connect the two SuperStack II Switch units using a Virtual LAN Trunk (VLT). For more information about VLTs, refer to "Connecting Common VLANs Between Switch Units" on page 5-3.

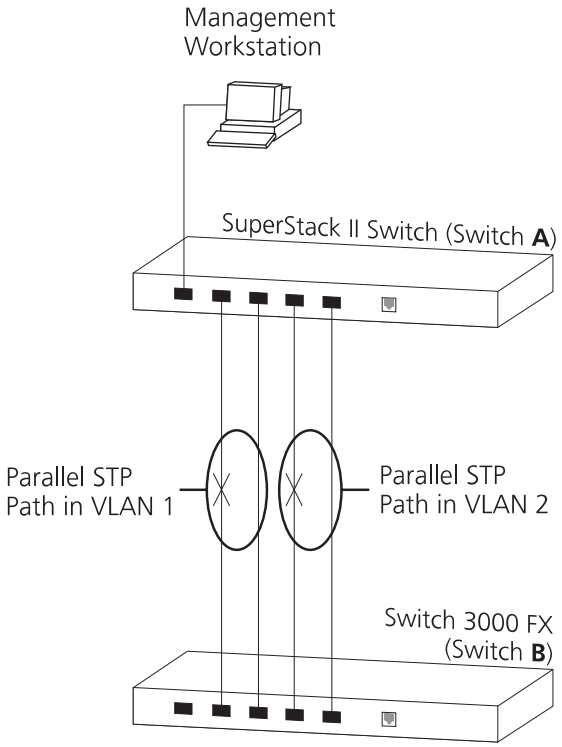
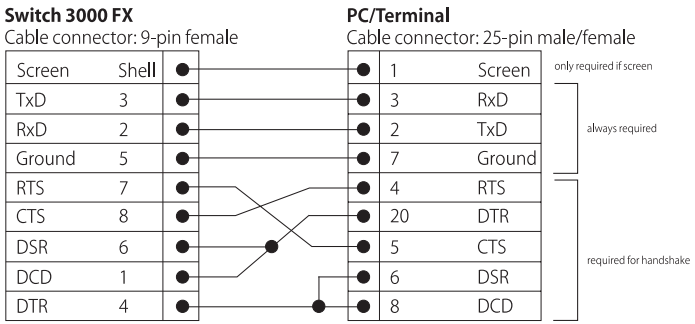


Figure C-1 Network configuration that results in loss of contact

D PIN-OUTS

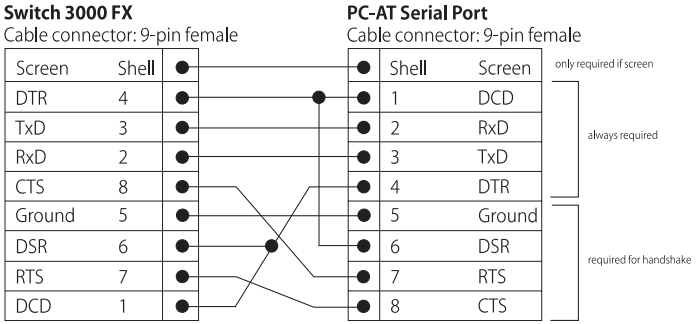
Null Modem Cable

9-pin to RS-232 25-pin



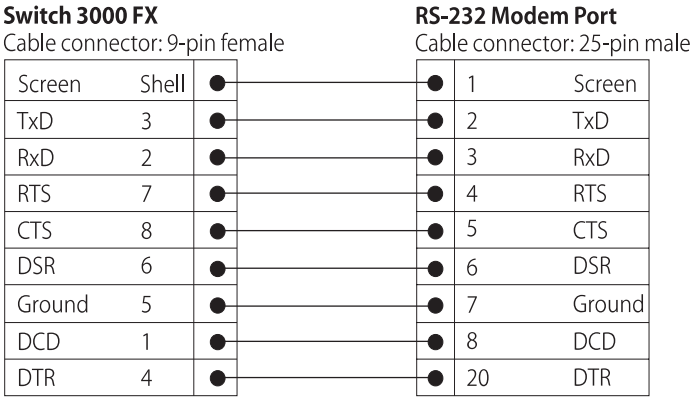
PC-AT Serial Cable

9-pin to 9-pin



Modem Cable

9-pin to RS-232 25-pin



RJ45 Pin Assignments

Ports configured as MDI

Pin Number	Signal	Function
1	TxData +	Transmit data
2	TxData -	Transmit data
3	RxData +	Receive data
4	Not Assigned	
5	Not Assigned	
6	RxData -	Receive data
7	Not Assigned	
8	Not Assigned	

Ports configured as MDIX

Pin Number	Signal	Function
1	RxData +	Receive data
2	RxData -	Receive data
3	TxData +	Transmit data
4	Not Assigned	
5	Not Assigned	
6	TxData -	Transmit data
7	Not Assigned	
8	Not Assigned	

E SWITCH 3000 FX TECHNICAL SPECIFICATIONS

Physical Dimensions	Height: 76mm (3.0in.) x Width: 483mm (19.0in.) x Depth: 300mm (12.0in.) Weight: 4.4kg (9.7lbs)
Environmental Requirements	
Operating Temperature	0–50°C (32–122°F)
Storage Temperature	-10–70°C (14–158°F)
Operating Humidity	10–95% relative humidity, non-condensing
Standards	EN60068 (IEC68)
Safety	
Agency Certifications	UL 1950, EN60950, CSA 22.2 No. 950
AC Protection	5A Time Delay Fuse
Electromagnetic Compatibility	EN55022 Class B*, FCC Part 15 Subpart B Class A, ICES-003 Class A, VCCI Class 2*, AS/NZS 3548 Class B*, EN 50082-1 * Category 5 screened cables must be used to ensure compliance with the Class B/Class 2 requirements of this standard. The use of unscreened cables (Category 5 for 100BASE-TX ports) complies with the Class A/Class 1 requirements.
Heat Dissipation	100W maximum (341.2 BTU/hour maximum)
Power Supply	
AC Line Frequency	50–60Hz
Input Voltage Options	100–120 / 200–240 VAC
Current Rating	3A (maximum) at 100 VAC / 2A (maximum) at 240 VAC

Standards Supported	SNMP	Protocols Used for Administration
	SNMP protocol (RFC 1157)	UDP (RFC 768)
	MIB-II (RFC 1213)	IP (RFC 791)
	Bridge MIB (RFC 1493)	ICMP (RFC 792)
	Repeater MIB (RFC 1516)	TCP (RFC 793)
	VLAN MIB (RFC 1573)	ARP (RFC 826)
	RMON MIB (RFC 1271 and RFC 1757)	TFTP (RFC 783)
	Terminal Emulation	BOOTP (RFC 951)
	Telnet (RFC 854)	

TECHNICAL SUPPORT

3Com provides easy access to technical support information through a variety of services. This appendix describes these services.

Information contained in this appendix is correct at time of publication. For the very latest, we recommend that you access 3Com Corporation's World Wide Web site.

Online Technical Services

3Com offers worldwide product support 24 hours a day, 7 days a week, through the following online systems:

- World Wide Web site
- 3Com Bulletin Board Service (3ComBBS)
- 3ComFacts℠ automated fax service
- 3ComForum on CompuServe® online service

World Wide Web Site

Access the latest networking information on 3Com Corporation's World Wide Web site by entering our URL into your Internet browser:

http://www.3Com.com/

This service features news and information about 3Com products, customer service and support, 3Com Corporation's latest news releases, *NetAge*® Magazine, technical documentation, and more.

3Com Bulletin Board Service

3ComBBS contains patches, software, and drivers for all 3Com products, as well as technical articles. This service is available via modem or ISDN 24 hours a day, 7 days a week.

Access by Analog Modem

To reach the service by modem, set your modem to 8 data bits, no parity, and 1 stop bit. Call the telephone number nearest you:

Country	Data Rate	Telephone Number
Australia	up to 14400 bps	61 2 9955 2073
Brazil	up to 14400 bps	55 11 547 9666
France	up to 14400 bps	33 1 6986 6954
Germany	up to 28800 bps	4989 62732 188
Hong Kong	up to 14400 bps	852 2537 5608
Italy (fee required)	up to 14400 bps	39 2 27300680
Japan	up to 14400 bps	81 3 3345 7266
Mexico	up to 28800 bps	52 5 520 7853
P. R. of China	up to 14400 bps	86 10 684 92351
Singapore	up to 14400 bps	65 534 5693

Country	Data Rate	Telephone Number
Taiwan	up to 14400 bps	886 2 377 5840
U.K.	up to 28800 bps	44 1442 438278
U.S.A.	up to 28800 bps	1 408 980 8204

Access by Digital Modem

ISDN users can dial in to 3ComBBS using a digital modem for fast access up to 56 Kbps. To access 3ComBBS using ISDN, use the following number:

(1) 408 654 2703

3ComFacts Automated Fax Service

3Com Corporation's interactive fax service, 3ComFacts, provides data sheets, technical articles, diagrams, and troubleshooting instructions on 3Com products 24 hours a day, 7 days a week.

Call 3ComFacts using your Touch-Tone telephone using one of these international access numbers:

Country	Telephone Number
Hong Kong	852 2537 5610
U.K.	44 1442 438279
U.S.A.	1 408 727 7021

Local access numbers are available within the following countries:

Country	Telephone Number
Australia	1 800 123853
Belgium	0800 71279
Denmark	800 17319
Finland	98 001 4444
France	05 90 81 58
Germany	0130 81 80 63
Italy	1678 99085

Country	Telephone Number
Netherlands	06 0228049
Norway	800 11062
Portugal	0505 442 607
Russia (Moscow only)	956 0815
Spain	900 964 445
Sweden	020 792954
U.K.	0800 626403

3ComForum on CompuServe Online Service

3ComForum contains patches, software, drivers, and technical articles about all 3Com products, as well as a messaging section for peer support. To use 3ComForum, you need a CompuServe account.

To use 3ComForum:

1. Log on to your CompuServe account.
2. Type **`go threecom`**
3. Press [Return] to see the 3ComForum main menu.

Support from Your Network Supplier

If additional assistance is required, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you contact your network supplier for assistance, have the following information ready:

- A list of system hardware and software, including revision levels
- Diagnostic error messages
- Details about recent configuration changes, if applicable

If you are unable to contact your network supplier, see the following section on how to contact 3Com.

Support from 3Com

If you are unable to receive support from your network supplier, technical support contracts are available from 3Com.

Contact your local 3Com sales office to find your authorized service provider using one of these numbers:

Regional Sales Office	Telephone Number
3Com Corporation	800 NET 3Com *or*
U.S.	1 408 764 5000
3Com ANZA	
East	61 2 9937 5000
West	61 3 9866 8022
3Com Asia Limited	
P. R. of China	86 10 68492 568 (Beijing)
	86 21 6374 0220 Ext 6115
Hong Kong	(Shanghai)
India	852 2501 1111
Indonesia	91 11 644 3974
Korea	62 21 523 9181
Malaysia	82 2 319 4711
Singapore	60 3 732 7910
Taiwan (R.O.C.)	65 538 9368
Thailand	886 2 377 5850
3Com Benelux B.V.	662 231 8151 4
Belgium	
Netherlands	32 725 0202
3Com Canada	31 30 6029700
Calgary	
Montreal	403 265 3266
Ottawa	514 683 3266
Toronto	613 566 7055
Vancouver	416 498 3266
3Com France	604 434 3266
3Com GmbH	33 1 69 86 68 00
Austria	
Czech/Slovak Republics	43 1 5134323
Germany	42 2 21845 800
	49 30 3498790 (Berlin)
Hungary	49 89 627320 (Munich)
Poland	36 1 250 83 41
Switzerland	48 22 6451351
3Com Ireland	41 31 996 14 14
3Com Japan	353 1 820 7077
	81 3 3345 7251

Regional Sales Office	Telephone Number
3Com Latin America	
Argentina	54 1 312 3266
Brazil	55 11 546 0869
Chile	56 2 633 9242
Colombia	57 1 629 4110
Mexico	52 5 520 7841
Peru	51 1 221 5399
Venezuela	58 2 953 8122
3Com Mediterraneo	
Italy	39 2 253011 (Milan) 39 6 5279941 (Rome)
3Com Middle East	971 4 349049
3Com Nordic AB	
Denmark	45 39 27 85 00
Finland	358 0 435 420 67
Norway	47 22 18 40 03
Sweden	46 8 632 56 00
3Com Russia	007 095 2580940
3Com South Africa	27 11 807 4397
3Com U.K. Limited	44 131 2478558 (Edinburgh) 44 161 8737717 (Manchester) 44 1628 897000 (Marlow)

Returning Products for Repair

Before you send a product directly to 3Com for repair, you must first obtain a Return Materials Authorization (RMA) number. Products sent to 3Com without RMA numbers will be returned to the sender unopened, at the sender's expense.

To obtain an RMA number, call or fax:

Location	Telephone Number	Fax Number
U.S.A. and Canada	1 800 876 3266, option 2	408 764 7120
Latin America	1 408 326 7801	408 764 7120
Europe, South Africa and Middle East	44 1442 438125	44 1442 435822
Elsewhere	1 408 326 7804	1 408 764 7120

02/06/97

GLOSSARY

10BASE-T

The IEEE 802.3 specification for Ethernet over Unshielded Twisted Pair (UTP) cabling.

100BASE-FX

100Mbps Ethernet implementation over fiber.

100BASE-TX

100Mbps Ethernet implementation over category 5 and Type 1 Twisted Pair cabling.

ageing

The automatic removal of dynamic entries from the Switch Database which have timed-out and are no longer valid.

ATM

Asynchronous Transfer Mode. A connection oriented transmission protocol based on fixed length cells (packets). ATM is designed to carry a complete range of user traffic, including voice, data and video signals.

backbone

The part of a network used as the primary path for transporting traffic between network segments.

bandwidth

Information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10Mbps, the bandwidth of Fast Ethernet is 100Mbps.

baud rate

The switching speed of a line. Also known as *line speed*.

BOOTP

The BOOTP protocol allows you to automatically map an IP address to a given MAC address each time a device is started. In addition, the protocol can assign the subnet mask and default gateway to a device.

bridge

A device that interconnects local or remote networks no matter what higher level protocols are involved. Bridges form a single logical network, centralizing network administration.

broadcast

A message sent to all destination devices on the network.

broadcast storm

Multiple simultaneous broadcasts that typically absorb available network bandwidth and can cause network failure.

console port

The port on the Switch accepting a terminal or modem connector. It changes the parallel arrangement of data within computers to the serial form used on data transmission links. This port is most often used for dedicated local management.

CSMA/CD

Channel access method used by Ethernet and IEEE 802.3 standards in which devices transmit only after finding the data channel clear for some period of time. When two devices transmit simultaneously, a collision occurs and the colliding devices delay their retransmissions for a random amount of time.

data center switching

The point of aggregation within a corporate network where a switch provides high-performance access to server farms, a high-speed backbone connection and a control point for network management and security.

Ethernet

A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks operate at 10Mbps using CSMA/CD to run over cabling.

Fast Ethernet

100Mbps technology based on the Ethernet/CD network access method.

forwarding

The process of sending a frame toward its destination by an internetworking device.

full duplex

A system which allows frames to be transmitted and received simultaneously and, in effect, doubles the potential throughput of a link.

IFM

Intelligent Flow Management. A means of holding packets back at the transmit port of the connected endstation. Prevents packet loss at a congested switch port.

IPX

Internetwork Packet Exchange. A protocol allowing communication in a NetWare network.

IP address

Internet Protocol address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with full-stops (periods), and is made up of a network section, an optional subnet section and a host section.

LAN

Local Area Network. A network of connected computing resources (such as PCs, printers, servers) covering a relatively small geographic area (usually not larger than a floor or building). Characterized by high data rates and low error rates.

latency

The delay between the time a device receives a frame and the time the frame is forwarded out of the destination port.

line speed

See *baud rate*.

main port

The port in a resilient link that carries data traffic in normal operating conditions.

MDI / MDIX

Medium Dependent Interface. A type of Ethernet twisted pair port connection: MDI ports connect to MDIX (cross-over) ports using straight-through twisted pair cabling; MDI-to-MDI and MDIX-to-MDIX links use cross-over twisted pair cabling.

MIB

Management Information Base. Stores a device's management characteristics and parameters. MIBs are used by the Simple Network Management Protocol (SNMP) to contain attributes of their managed systems. The Switch contains its own internal MIB.

multicast

Single packets copied to a specific subset of network addresses. These addresses are specified in the destination-address field of the packet.

PACE

Priority Access Control Enabled. 3Com's innovative technology which works in conjunction with a switch to control the latency and jitter associated with the transmission of multimedia traffic over Ethernet and Fast Ethernet.

POST

Power On Self Test. An internal test that the Switch carries out when it is powered-up.

protocol

A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.

resilient link

A pair of ports that can be configured so that one will take over data transmission should the other fail. See also *main port* and *standby port*.

RJ45

Standard 8-wire connectors for IEEE 802.3 10BASE-T networks.

RMON

Remote Monitoring. Subset of SNMP MIB II allows monitoring and management capabilities by

addressing up to ten different groups of information.

RPS

Redundant Power System. Part of the SuperStack® II product range, provides a backup source of power when connected to the Switch.

server farm

A cluster of servers in a centralized location serving a wide user population.

SLIP

Serial Line Internet Protocol. A protocol which allows IP to run over a serial line connection.

SmartAgent

Intelligent management agents in devices and logical connectivity systems that reduce the computational load on the network management station and reduce management-oriented traffic on the network.

SNMP

Simple Network Management Protocol. A protocol originally designed to be used in managing TCP/IP internets. SNMP is presently implemented on a wide range of computers and networking equipment and may be used to manage many aspects of network and endstation operation.

Spanning Tree Protocol (STP)

A bridge-based system for providing fault tolerance on networks. STP works by allowing you to implement parallel paths for network traffic, and ensure that redundant paths are disabled when the main paths are operational and enabled if the main paths fail.

standby port

The port in a resilient link that will take over data transmission if the main port in the link fails.

STP

See *Spanning Tree Protocol (STP)*.

switch

A device which filters, forwards and floods frames based on the frame's destination address. The switch learns the addresses associated with each switch port and builds tables based on this information to be used for the switching decision.

TCP/IP

A layered set of communications protocols providing Telnet terminal emulation, FTP file transfer, and other services for communication among a wide range of computer equipment.

Telnet

A TCP/IP application protocol that provides virtual terminal service, letting a user log in to another computer system and access a host as if the user were connected directly to the host.

TFTP

Trivial File Transfer Protocol. Allows you to transfer files (such as software upgrades) from a remote device using your Switch unit's local management capabilities.

Transcend®

3Com's umbrella management system used to manage all of 3Com's networking solutions.

UDP

User Datagram protocol. An Internet standard protocol that allows an application program on one device to send a datagram to an application program on another device.

VLAN

Virtual LAN. A group of location- and topology-independent devices that communicate as if they are on a common physical LAN.

VLT

Virtual LAN Trunk. A Switch-to-Switch link which carries traffic for all the VLANs on each Switch.

VT100

A type of terminal which uses ASCII characters. VT100 screens have a text-based appearance.

INDEX

Numerics

100BASE-FX port 1-2, 1-9
100BASE-TX port 1-2, 1-10
3Com Bulletin Board Service (3ComBBS) F-1
3Com sales offices F-3
3Com URL F-1
3ComFacts F-2
3ComForum F-2

A

Access Level field 4-3
access rights B-1
Active Port field 4-20, 4-21
ageing entries 4-15
ageing time, specifying 4-10
agent software version number 6-8
alarm actions 5-27
alarm settings, default 5-28
Alarms (RMON group) 5-23, 5-25
Asynchronous Transfer Mode. *See* ATM
ATM Module 1-1
ATM networks, extending VLANs into 5-5
audit log 5-28
Auto Config field 4-24
auto configuration 4-24
auto logout 3-12
Auto Logout screen 3-12
AutoSelect VLAN Mode 5-4
  specifying 5-11

B

Backup VLAN Server IP Address field 5-10
baud rate. *See* line speed
Boot Software Version field 6-8
BOOTP Select field 3-10
BOOTP server 1-13, 3-6
BPDUs. *See* Bridge Protocol Data Units
Bridge Forward Delay field 5-19
Bridge Hello Time field 5-19
Bridge Identifier 5-14
Bridge Max Age field 5-19
Bridge Priority field 5-19
Bridge Protocol Data Units 5-14
Broadcast Storm Control field 4-13
Bulletin Board Service F-1

C

cable
  maximum length 1-2, 1-9, 2-2
  pin-outs D-1
Capture (RMON group) 5-23, 5-26
Char Size field 4-25
Community String field 4-3, 4-5, 4-23
community strings
  changing 4-5
  entering 4-3
  role in trap setup 4-23
  VLAN server 5-10
Community-SNMP field 4-6
CompuServe® F-2
Connection Type field 4-24
console port 1-11
  auto-configuration 4-24
  connecting equipment to 2-7
  connection type 4-24
  disabling access 4-6
  setting up 4-24
  speed 4-24
Console Port field 4-6
Console Port Setup screen 4-24
conventions
  notice icons, About This Guide 2
  text, About This Guide 2
counters
  Bandwidth Used (port) 6-3
  Broadcast Frame Bandwidth (port) 6-3
  Broadcast Received (port traffic) 6-4
  Collisions (port traffic) 6-4
  CRC Align Errors (port error) 6-6
  Errors (port traffic) 6-5
  Errors (port) 6-3
  Errors (summary) 6-2
  Fragments (port traffic) 6-5
  Frame Size Analysis (port traffic) 6-5
  Frames Filtered (port traffic) 6-5
  Frames Filtered (summary) 6-2
  Frames Forwarded (port traffic) 6-5
  Frames Forwarded (port) 6-3
  Frames Forwarded (summary) 6-2
  Frames Received (port traffic) 6-4
  Frames Received (summary) 6-2
  Frames Transmitted (port traffic) 6-4
  Frames Transmitted (summary) 6-2
  IFM Count (port traffic) 6-5
  Jabbers (port error) 6-7
  Late Events (port error) 6-6
  Long Frames (port error) 6-6
  Multicasts Received (port traffic) 6-4
  Multicasts Received (summary) 6-2

Multicasts Transmitted (summary) 6-2
Octets Received (port traffic) 6-4
Octets Transmitted (port traffic) 6-4
resetting to zero 6-2, 6-5, 6-7
Short Events (port error) 6-6
Create User screen 4-3

D

Data Link Protocol field 3-10
Database Entries field 4-16
database. *See* Switch Database
DCD Control field 4-24
default
passwords 3-7
router 3-10
settings 1-12
users 3-7
Default RMON Host/Matrix field 4-10
Default Router field 3-10
Default VLAN 5-3
Delete Users screen 4-4
Designated Bridge field 5-21
Designated Bridge Port 5-14
Designated Cost field 5-21
Designated Port field 5-20
Designated Root field 5-18, 5-20
Destination field 4-28
Device IP Address field 3-10
Device SubNet Mask field 3-10
Disable Interactive Access field 4-12
Downlink Module. *See* Plug-in Module
DSR Control field 4-24
Duplex Mode field 4-10, 4-12

E

Edit User screen 4-5
Ethernet address label 1-11
Events (RMON group) 5-24, 5-26

F

Falling Action field 4-14
Falling Threshold% field 4-13
Fast Boot tests 3-9
Fast Ethernet configuration rules 2-2
Fast Start field 5-21
Fault Log screen 6-9
Fault Log, interpreting 6-9
Fault Number field 6-9
fax service. *See* 3ComFacts
fields
Access Level 4-3
Active Port 4-20, 4-21
Auto Config 4-24
Backup VLAN Server IP Address 5-10
Boot Software Version 6-8
BOOTP Select 3-10
Bridge Forward Delay 5-19
Bridge Hello Time 5-19
Bridge Max Age 5-19
Bridge Priority 5-19
Broadcast Storm Control 4-13
Char Size 4-25
Community String 4-3, 4-5, 4-23
Community-SNMP 4-6
Connection Type 4-24
Console Port 4-6
Data Link Protocol 3-10
Database Entries 4-16
DCD Control 4-24
Default RMON Host/Matrix 4-10
Default Router 3-10
Designated Bridge 5-21
Designated Cost 5-21
Designated Port 5-20
Designated Root 5-18, 5-20
Destination 4-28
Device IP Address 3-10
Device SubNet Mask 3-10
Disable Interactive Access 4-12
DSR Control 4-24
Duplex Mode 4-10, 4-12
Falling Action 4-14
Falling Threshold% 4-13
Fast Start 5-21
Fault Number 6-9
File Name 4-28
Flow Control 4-24
Forward Delay 5-19
Fwd Transitions 5-21
Hardware Version 6-8
Hello Time 5-18
Hold Time 5-19
Intelligent Flow Management 4-11
IP or IPX Address 4-23
IPX Network 3-10
Last Reset Type 6-8
Link State 4-11, 4-19
Lost Links 4-11
MAC Address 3-9, 4-16
Main Port 4-21
Main Port ID 4-19
Management Level 4-7
Max Age 5-18
Media Type 4-11, 4-19
New Password 4-5
Node 3-10
Number of Resets 6-8
Old Password 4-5
Oversize Frames 4-10
PACE 4-9
Pair Enable 4-20, 4-22
Pair State 4-19, 4-21
Parity 4-25
Password 4-3
Path Cost 5-21
Permanent 4-16
Plug-in Module Type 4-10
Poll Period 5-10
Port Enable 5-21
Port Number 4-16
Port Speed 4-11
Port State 4-11

Power On Self Test Type 3-9
Power Supply 4-10
Priority 5-21
Remote Telnet 4-6
Reset Count 6-9
Rising Action 4-13
Rising Threshold% 4-13
Root Cost 5-18
Root Port 5-19
Round Trip Time 6-10
SDB Ageing Time 4-10
Server Address 4-28
SLIP Address 3-10
SLIP Subnet Mask 3-10
Spanning Tree 4-10
Speed 4-25
Standby Links Available 4-19
STANDBY Port 4-21
Standby Port ID 4-19
Stop Bit 4-25
STP State 5-20
sysName 4-9
System Up Time 6-8
Target Address 6-10
Throttle 4-23, 5-10
Time Since Topology Change 5-19
Topology Changes 5-18
Transceiver Module Type 4-10
Type 5-8
Unit Name 4-9
Upgradable Software Version 6-8
User Name 4-3, 4-5
VLAN Configuration Mode 4-10, 4-13
VLAN ID 5-9, 5-18
VLAN Membership 5-8
VLAN Server Community String 5-10
VLAN Server IP Address 5-10
VLT Mode 4-12
File Name field 4-28
Filter (RMON group) 5-23, 5-26
Flow Control field 4-24
Forward Delay field 5-19
full duplex 1-3
configuration rules 2-2
enabling and disabling 4-10, 4-12
fuse, changing A-3
Fwd Transitions field 5-21

H

Hardware Version field 6-8
Hello BPDUs 5-15
Hello Time 5-14
Hello Time field 5-18
History (RMON group) 5-22, 5-25
Hold Time field 5-19
Hosts (RMON group) 5-23, 5-26
Hosts and Matrix RMON sessions 4-10
Hosts Top N (RMON group) 5-23, 5-26

I

IFM. *See* Intelligent Flow Management
Initialization screen 4-27
initializing the Switch 4-27
installing the Switch 2-4
Intelligent Flow Management 1-3
Intelligent Flow Management field 4-11
Interactive Access, disabling 4-12
IP address
backup VLAN server 5-10
default router 3-10
entering 1-13
format 3-2
Switch 3-10
VLAN server 5-10
IP or IPX Address field 4-23
IP protocol 1-12
IPX address 1-13
IPX Network field 3-10
IPX protocol 1-12

K

keyboard shortcuts 3-5

L

Last Reset Type field 6-8
Learning state, transitions from 5-21
LEDs 1-9
line speed 4-25
Link State field 4-11, 4-19
Local Security screen 4-6
logging off 3-12
logging on 3-7
Logon screen 3-7
Lost Links field 4-11

M

MAC Address field 3-9, 4-16
MAC address label 1-11
Main Banner screen 3-6
Main Menu screen 3-8
MAIN Port field 4-21
Main Port ID field 4-19
management agent version number 6-8
Management Level field 4-7
Management Setup screen 3-9
Matrix (RMON group) 5-23, 5-26
Max Age 5-15
Max Age field 5-18
Media Type field 4-11, 4-19

N

network supplier support F-3
New Password field 4-5
Node field 3-10
non-ageing entries 4-15
non-routable protocols 5-5

Number of Resets field 6-8

O

Old Password field 4-5
on-line technical services F-1
Oversize Frames field 4-10

P

PACE 1-4
  disabling Interactive Access for a port 4-12
  enabling and disabling 4-9
PACE field 4-9
Pair Enable field 4-20, 4-22
Pair State field 4-19, 4-21
Parity field 4-25
Password field 4-3
passwords
  changing 4-5
  default 3-7
  forgetting 4-5
  new 4-3
Path Cost field 5-21
path costs, default 5-14
permanent entries 4-15
  displaying 4-16
  specifying 4-17
Permanent field 4-16
pin assignments
  modem cable D-2
  null modem cable D-1
  RJ45 D-2
  serial cable D-1
Plug-in Module 1-2
  slot 1-11
Plug-in Module Type field 4-10
Poll Period field 5-10
port
  100BASE-FX 1-2, 1-9
  100BASE-TX 1-2, 1-9
  console 1-11
  enabling and disabling 4-11
  speed 4-11
  statistics 6-3
Port Enable field 5-21
Port Error Analysis screen 6-6
Port Number field 4-16
Port Resilience screen 4-19
Port Setup screen 4-11
Port Speed field 4-11
Port State field 4-11
Port Statistics screen 6-3
Port STP screen 5-20
Port Traffic Statistics screen 6-4
Port VLAN Mode 5-4
POST. *See* Power On Self Test
Power On Self Test Type field 3-9
power supply 1-11
Power Supply field 4-10
powering-up 2-6
Priority field 5-21
problem solving C-1

Q

quick start for SNMP users 1-13

R

rack mounting 2-4
Redundant Power System. *See* RPS
Remote Monitoring. *See* RMON
Remote Poll screen 6-10
remote polling 6-10
Remote Telnet field 4-6
reset button 1-11
Reset Count field 6-9
Reset screen 4-26
resets
  number of 6-8
  type 6-8
resetting the Switch 4-26
resilient link pair 4-18
resilient links 1-3
  configuring 4-19
  creating 4-20
  deleting 4-20
  rules 4-18
  setting up 4-18
  viewing 4-19
returning products for repair F-4
Rising Action field 4-13
Rising Threshold% field 4-13
RMON 5-22
  alarm actions 5-27
  benefits 5-24
  default alarm settings 5-28
  features supported 5-25
  groups supported 5-25
  probe 5-22
Root Bridge 5-14
Root Cost field 5-18
Root Path Cost 5-14
Root Port field 5-19
Round Trip Time field 6-10
RPS 1-11
  connecting 2-6

S

safety information
  English A-1
  French A-4
  German A-7
screens 4-1
  access rights B-1
  Auto Logout 3-12
  Console Port Setup 4-24
  Create User 4-3
  Delete Users 4-4
  Edit User 4-5
  Fault Log 6-9

Initialization 4-27
Local Security 4-6
Logon 3-7
Main Banner 3-6
Main Menu 3-8
Management Setup 3-9
Port Error Analysis 6-6
Port Resilience 4-19
Port Setup 4-11
Port Statistics 6-3
Port STP 5-20
Port Traffic Statistics 6-4
Remote Poll 6-10
Reset 4-26
Software Upgrade 4-28
Status 6-8
Summary Statistics 6-2
Switch Management 4-7
Trap Setup 4-23
Unit Database View 4-16
Unit Resilience Summary 4-21
Unit Setup 4-9
User Access Levels 4-2
VLAN Server 5-10
VLAN Setup 5-8
VLAN STP 5-18
SDB Ageing Time field 4-10
serial number, location on unit 1-11
serial port. *See* console port
Server Address field 4-28
SLIP Address field 3-10
SLIP Subnet Mask field 3-10
SNMP 1-12, 3-6
Community 4-6
quick start 1-13
socket
power 1-11
RPS 1-11
Software Upgrade screen 4-28
software version number 6-8
Spanning Tree field 4-10
Spanning Tree Protocol. *See* STP
specifications, system E-1
Speed field 4-25
standards supported E-2
Standby Links Available field 4-19
STANDBY Port field 4-21
Standby Port ID field 4-19
statistics 6-1
counters. *See* counters
port 6-3
port error 6-6
port traffic 6-4
summary 6-2
Statistics (RMON group) 5-22, 5-25
Status screen 6-8
Stop Bit field 4-25
STP 1-4, 5-12
Bridge Identifier 5-14
Bridge Protocol Data Units 5-14
configurations 5-16
configuring port properties 5-20
configuring VLAN properties 5-18
default path costs 5-14
Designated Bridge Port 5-14
enabling and disabling 4-10, 5-17
Hello BPDUs 5-15
Hello Time 5-14
Max Age 5-15
Root Bridge 5-14
Root Path Cost 5-14
STP State field 5-20
subnet mask, device 3-10
Summary Statistics screen 6-2
Switch 3000 FX 1-1
configuration examples 1-6
dimensions E-1
features 1-1
front view 1-8
initializing 4-27
installing 2-4
LEDs 1-9
logging off 3-12
logging on 3-7
management setup 3-9
port setup 4-11
positioning 2-1
powering-up 2-6
rack mounting 2-4
rear view 1-10
resetting 4-26
size E-1
stacking with other units 2-4
unit defaults 1-12
unit setup 4-9
upgrading software 4-28
wall mounting 2-5
weight E-1
Switch Database 4-15
adding an entry 4-17
ageing entries 4-15
configuring 4-16
deleting an entry 4-17
non-ageing entries 4-15
permanent entries 4-15
searching 4-17
traps 4-15
Switch Management screen 4-7
sysName field 4-9
system specifications E-1
System Up Time field 6-8

T

Target Address field 6-10
technical support F-1
3Com URL F-1
Bulletin Board Service F-1
fax service F-2
network suppliers F-3
product repair F-4
using CompuServe F-2
Telnet 3-2, 4-6
Throttle field 4-23, 5-10
time since reset 6-8

Time Since Topology Change field 5-19
Token Ring frames, encapsulation of 4-10
Topology Changes field 5-18
Transceiver Module 1-2
  slot 1-11
Transceiver Module Type field 4-10
Trap Setup screen 4-23
traps
  community strings 4-23
  setting up 4-23
  throttle 4-23
trouble-shooting C-1
Type field 5-8

U

Unit Database View screen 4-16
unit defaults 1-12
Unit Name field 4-9
Unit Resilience Summary screen 4-21
Unit Setup screen 4-9
Upgradable Software Version field 6-8
upgrading software 4-28
URL F-1
User Access Levels screen 4-2
User Name field 4-3, 4-5
users
  access levels 4-6
  changing names 4-5
  creating 4-3
  default 3-7
  deleting 4-4
  editing 4-5
  names 4-3
  passwords 4-3
  setting up 4-2

V

version number
  boot software 6-8
  hardware 6-8
  upgradable software 6-8
Virtual LAN Trunks. *See* VLTs
Virtual LANs. *See* VLANs
VLAN Configuration Mode field 4-10, 4-13
VLAN ID field 5-9, 5-18
VLAN Membership field 5-8
VLAN Server 5-4
VLAN Server Community String field 5-10
VLAN Server IP Address field 5-10
VLAN Server screen 5-10
VLAN Setup screen 5-8
VLAN STP screen 5-18
VLANs 1-4, 5-1
  assigning ports 5-9
  AutoSelect VLAN Mode 5-4
  Default 5-3
  extending into an ATM network 5-5
  Port VLAN Mode 5-4
  setting up 5-8
  using non-routable protocols 5-5
  using unique MAC addresses 5-5
  VLTs 5-8
VLT Mode field 4-12
VLTs 5-3, 5-8, 5-9
VT100 interface
  accessing 3-1
  definition 1-12
  logging on 3-7
  navigating 3-4
VT100 terminal, connecting 2-7

W

wall mounting 2-5
World Wide Web (WWW) F-1

Z

zeroing screen counters 6-2, 6-5, 6-7

3Com Corporation LIMITED WARRANTY

HARDWARE

3Com warrants its hardware products to be free from defects in workmanship and materials, under normal use and service, for the following lengths of time from the date of purchase from 3Com or its Authorized Reseller:

Network adapters	Lifetime
Other hardware products (unless otherwise specified above)	1 year
Spare parts and spare kits	90 days

If a product does not operate as warranted above during the applicable warranty period, 3Com shall, at its option and expense, repair the defective product or part, deliver to Customer an equivalent product or part to replace the defective item, or refund to Customer the purchase price paid for the defective product. All products that are replaced will become the property of 3Com. Replacement products may be new or reconditioned. Any replaced or repaired product or part has a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

3Com shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to 3Com for repair, whether under warranty or not.

SOFTWARE

3Com warrants that the software programs licensed from it will perform in substantial conformance to the program specifications therefor for a period of ninety (90) days from the date of purchase from 3Com or its Authorized Reseller. 3Com warrants the media containing software against failure during the warranty period. No updates are provided. 3Com's sole obligation with respect to this express warranty shall be (at 3Com's discretion) to refund the purchase price paid by Customer for any defective software products, or to replace any defective media with software which substantially conforms to 3Com's applicable published specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials. 3Com makes no warranty or representation that its software products will work in combination with any hardware or applications software products provided by third-parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third-party products listed in the 3Com software product documentation or specifications as being compatible, 3Com will make reasonable efforts to provide compatibility, except where the noncompatibility is caused by a "bug" or defect in the third-party's product.

STANDARD WARRANTY SERVICE

Standard warranty service for *hardware* products may be obtained by delivering the defective product, accompanied by a copy of the dated proof of purchase, to 3Com's Corporate Service Center or to an Authorized 3Com Service Center during the applicable warranty period. Standard warranty service for *software* products may be obtained by telephoning 3Com's Corporate Service Center or an Authorized 3Com Service Center, within the warranty period. Products returned to 3Com's Corporate Service Center must be pre-authorized by 3Com with a Return Material Authorization (RMA) number marked on the outside of the package, and sent prepaid, insured, and packaged appropriately for safe shipment. The repaired or replaced item will be shipped to Customer, at 3Com's expense, not later than thirty (30) days after receipt of the defective product by 3Com.

WARRANTIES EXCLUSIVE

IF A 3COM PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, CUSTOMER'S SOLE REMEDY FOR BREACH OF THAT WARRANTY SHALL BE REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. TO THE FULL EXTENT ALLOWED BY LAW, THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, TERMS, OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES, TERMS, OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND SATISFACTORY QUALITY. 3COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, OR USE OF ITS PRODUCTS.

3COM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

LIMITATION OF LIABILITY

TO THE FULL EXTENT ALLOWED BY LAW, 3COM ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, EVEN IF 3COM OR ITS AUTHORIZED RESELLER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT 3COM'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

Some countries, states, or provinces do not allow the exclusion or limitation of implied warranties or the limitation of incidental or consequential damages for certain products supplied to consumers or the limitation for personal injury, so the above limitations and exclusions may be limited in their application to you. This warranty gives you specific legal rights which may vary depending on local law.

GOVERNING LAW

This Limited Warranty shall be governed by the laws of the state of California.

3Com Corporation,
5400 Bayfront Plaza, Santa Clara, CA 95052-8145 (1) (408) 764-5000

9/1/96

ELECTRO-MAGNETIC COMPATIBILITY STATEMENTS

FCC STATEMENT

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference to radio communications, in which case the user will be required to correct the interference at their own expense.

CSA STATEMENT

This Class A digital apparatus meets all requirements of the Canadian interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

VCCI STATEMENT

この装置は、第二種情報処理装置(住宅地域又はその隣接した地域において使用されるべき情報処理装置)で住宅地域での電波障害防止を目的とした情報処理装置等電波障害自主規制協議会(ＶＣＣＩ)基準に適合しております。

しかし、本装置をラジオ、テレビジョン受信機に近接してご使用になると、受信障害の原因となることがあります。

取扱説明書に従って正しい取り扱いをして下さい 。

INFORMATION TO THE USER

If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna.
- Relocate the equipment with respect to the receiver.
- Move the equipment away from the receiver.
- Plug the equipment into a different outlet so that equipment and receiver are on different branch circuits.

If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions. The user may find the following booklet prepared by the Federal Communications Commission helpful:

How to Identify and Resolve Radio-TV Interference Problems

This booklet is available from the U.S. Government Printing Office, Washington, DC 20402, Stock No. 004-000-00345-4.

In order to meet FCC emissions limits, this equipment must be used only with cables which comply with IEEE 802.3.